
**UFF - UNIVERSIDADE FEDERAL FLUMINENSE
ESCOLA DE ENGENHARIA
MESTRADO EM ENGENHARIA DE TELECOMUNICAÇÕES**

ELOY TAVARES MENDES

**AVALIAÇÃO DOS SERVIÇOS VoIP
EM LINKS DE BAIXA CAPACIDADE COM
TRÁFEGO COMPARTILHADO DE DADOS.**

**Niterói
2011**

ELOY TAVARES MENDES

**AVALIAÇÃO DOS SERVIÇOS VoIP
EM LINKS DE BAIXA CAPACIDADE COM
TRÁFEGO COMPARTILHADO DE DADOS.**

Dissertação apresentada ao Programa de Pós-Graduação “*Stricto Sensu*” em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do título de Mestre. Área de concentração: Sistemas de Telecomunicações.

Orientador:
Prof. Carlos Alberto Malcher Bastos, DSc

Niterói
2011

Ficha Catalográfica elaborada pela Biblioteca da Escola de Engenharia e Instituto de Computação da UFF

M538 Mendes, Eloy Tavares.

Avaliação dos serviços VoIP em links de baixa capacidade com tráfego compartilhado de dados FTP / Eloy Tavares Mendes. – Niterói, RJ : [s.n.], 2011.

248 f.

Dissertação (Mestrado em Engenharia de Telecomunicações) - Universidade Federal Fluminense, 2011.

Orientador: Carlos Alberto Malcher Bastos.

1. Sistema de telefonia. 2. Telefonia pela Internet. 3. Qualidade de serviço. 4. Avaliação de desempenho. I. Título.

CDD 621.385

ELOY TAVARES MENDES

AVALIAÇÃO DOS SERVIÇOS VoIP EM LINKS DE BAIXA CAPACIDADE COM TRÁFEGO COMPARTILHADO DE DADOS.

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do grau de Mestre. Área de concentração: Sistemas de Telecomunicações.

Aprovada em 1º de Setembro de 2011

BANCA EXAMINADORA

Carlos A. Malcher Bastos

Prof. Carlos Alberto Malcher Bastos, D.Sc. – Orientador
Universidade Federal Fluminense - UFF

João Marcos Meirelles da Silva

Prof. João Marcos Meirelles da Silva, D.Sc.
Universidade Federal Fluminense - UFF

Anilton Salles Garcia

Prof. Anilton Salles Garcia, D.Sc.
Universidade Federal do Espírito Santo - UFES

Reconhecimento de Assinatura
Reconheço por semelhança a assinatura de

João Marcos Meirelles da Silva
Rio de Janeiro, 11/11/2011
Petrônio Antonio da Silva
Consul Geral

Niterói
2011



CARTÓRIO DO 2º OFÍCIO DE NITERÓI - RUA ALM. TEFFÉ 645 LOJA 101
Reconheço a(s) firma(s) por SEMELHANÇA:
CARLOS ALBERTO MALCHER BASTOS
NITERÓI, 11/11/2011 Total: R\$ 5,27 Recolhim.: R\$ 1,21
Em test. _____ da verdade. Conf. por: _____
THALES RIBEIRO PEREIRA

Dedicatória

Não seria possível a materialização do presente trabalho, se para o efeito eu não pudesse contar com a prestimosa colaboração de pessoas que desde há primeira hora se prontificaram a apoiar-me de forma incondicional. Algumas dessas pessoas chegaram mesmo a consentir sacrifícios para que hoje eu possa estar em condições de o apresentar. Assim, passo a dedicar esta obra às seguintes pessoas:

*- À minha querida e amada esposa, **Embelina da Veiga**, minha companheira e cúmplice nessa caminhada há já alguns anos e que sempre esteve do meu lado nos momentos bons e difíceis, dando sempre o melhor de si, muitas vezes a custo de muitos sacrifícios, para a prossecução desse objetivo. Ela, desde logo, acreditou em mim tendo demonstrando de forma íntegra e incondicional o seu apoio moral e muita compreensão ao longo desses anos difíceis mas muito gratificantes.*

*“Não espere por uma crise para descobrir o que é importante em sua vida” – **Platão***

*“A alegria está na luta, na tentativa, no sofrimento envolvido. Não na vitória propriamente dita.” – **Mahatma Gandhi***

*- A minha princesinha de cinco aninhos – minha linda filha **Lucieny Rosy da Veiga Tavares** – pelos períodos que estive longe dela. Ela é, sem dúvida, a pessoa que mais se sacrificou por mim. Guardarei para sempre na minha memória os desabafos inocentes mais sinceros que ela fazia com a mãe a propósito das minhas ausências. Certa vez, ela disse para a mãe: “Mãe não gosto de ficar com saudades do meu pai, porque se não fico triste”. Essas saudades foram, no entanto, reduzidas, graças à telefonia VoIP que me permitiu, religiosamente, escutar diariamente ao telefone a sua meiga voz dizendo em primeira mão, de entre outras coisas: “Estou com saudades tuas, Eloy...”.*

*O verdadeiro significado da vida reside na nossa tentativa de compreender o pensamento ingênuo, “inconsequente” e mui verdadeiro de uma criança – **Eloy Tavares***

*- Aos **meus queridos pais e ilustres irmãos**, pelas instruções da vida que me proporcionaram, pelo zelo, pelo engajamento, pela força e tenacidade que me transmitiram e, acima de tudo, pela enorme confiança que sempre depositaram em mim.*

*“Os homens existem uns para os outros; logo, ou instrua-os ou suporta-os” – **Marco Aurélio***

*- Finalmente, dedico esta dissertação **a todos aqueles** que embarcaram comigo neste sonho e acreditaram piamente na minha chegada a esta nova meta da minha vida académica.*

*“Nenhum vento sopra a favor de quem não sabe para onde ir” – **Sêneca***

*“Há quem passa pelo bosque e só veja lenha para a fogueira” – **Tolstói***

*“I have a dream (...) –
Eu tenho um sonho (...)”
– **Rev. Dr. Martin Luther King Jr***

*“As coisas não são boas ou ruins; o pensamento é que as faz assim”
– **William Shakespeare***

Agradecimentos

Na expectativa de ter chegado com sucesso ao fim de mais uma etapa da minha vida acadêmica, sinto-me na obrigação de expressar os meus sinceros votos de agradecimentos a todos aqueles que direta ou indiretamente contribuíram para a elaboração dessa dissertação. De entre eles, gostaria de salientar o nome daqueles que mais se envolveram neste processo, acreditando e fazendo tornar realidade esse trabalho. Entretanto, ao apontar o nome de alguns corro o risco de omitir o nome de outros. Se isso acontecer, eu gostaria de apresentar, desde já, as minhas sinceras desculpas. Assim, o meu especial agradecimento vai para as seguintes pessoas:

- Em primeira mão eu agradeço a Deus que tem iluminado a minha mente e a de todos aqueles que fizeram com que esse trabalho tornasse realidade. Deus seja louvado!

- **Ao Sr. Prof. Dr. Carlos Alberto Malcher Bastos** pela orientação, pela cooperação que mantivemos ao longo desse tempo, e pelos aconselhamentos extra-acadêmicos.

- Aos funcionários e amigos do Centro de Referência Tecnológica (CRT) da OP (Operadora de Telecomunicações) nomeadamente, **Mestre Eng. Walderson Vidal, Mestrando Eng. Carlos Terra, Mestrando e Colega Suzana Domingues**, entre outros, por participarem tecnicamente dos testes realizados no referido pólo tecnológico da Operadora.

- Ao **Sr. Prof. Dr. Anilton Salles** (UFES) que chegou a aceitar de bom grado ser meu co-orientador técnico, embora não chegou a sê-lo.

- Ao **Sr. Eng. Milton Flores** do laboratório GETCCOM, pelo agradável convívio que tivemos; à **Sr^a. Sulamita Silva**, então secretária do laboratório, pelas nossas conversas simples e afáveis; aos demais elementos do GETCCOM e à **Doutoranda Sr^a Vandira Pinheiros** pela preocupação que demonstrou em relação à minha dissertação, minha estadia no Brasil etc.

- Ao amigo e colega **Mestre Eng. Alex Galheano** e ao laboratório da FIRJAN, por ter concedido equipamentos e espaço para realização de alguns testes complementares.

- Ao amigo e colega **Mestrando Eng. Jailton Neves** da Oi, por ter participado ativamente de alguns testes no Laboratório da Operadora de Telecomunicações - LOP.

- À toda a minha família (**Meus Pais, Irmãos, Esposa e Filha**) pela confiança, incentivo, força e apoio moral que me dispensaram até a presente data, em particular o irmão **Agnelo Mendes** pelos sábios conselhos que me tem dado e por ter aceite gentilmente fazer a revisão do texto desta dissertação. A todos o meu muito obrigado. Até um dia se Deus quiser!

“As pessoas que vencem neste mundo são as que procuram as circunstâncias de que precisam e, quando não as encontram, as criam.” – BERNARD SHAW

SUMÁRIO

LISTA DAS ABREVIATURAS.....	xiv
RESUMO	xvii
ABSTRACT.....	xviii
1 - CAPÍTULO I: INTRODUTÓRIO.....	19
1.1 - Introdução.....	19
1.1.1 - Estrutura da dissertação.....	24
2 - CAPÍTULO II – REDES FRAME RELAY E RECOMENDAÇÃO SEGUNDO O PADRÃO FRAME RELAY FORUM v12 (FRF.12).....	27
2.1 - REDES FRAME RELAY	27
2.1.1 - Frame Relay - Conceito:	27
2.1.2 - Características do Frame Relay	28
2.1.3 - Algumas vantagens do Frame Relay:.....	29
2.1.4 - Estrutura de cabeçalho Frame Relay	30
2.1.5 - Interligação de LANs	31
2.1.6 - Controle de Tráfego em Frame Relay	33
2.1.7 - Controle de Congestionamento	34
2.1.8 - Moldagem e Policiamento de Tráfego	35
2.1.9 - Moldagem Genérica	35
2.2 - FRAME RELAY FORUM v12 (FRF.12).....	38
2.2.1 - Implementação de LFI em acesso Frame Relay (FR).....	39
2.2.2 - Multilink PPP	40
2.2.3 - LFI Especificação - Frame Relay Fórum v12 (FRF.12).....	40
2.2.4 - Técnicas de Fragmentação e Intercalação á Nível de Enlace FRF.12	41
3 - CAPÍTULO III – CARACTERÍSTICAS DOS SOFTWARES DE MEDIÇÕES	48
3.1 - MGEN - (MultiGenerator) Free Software.....	48
3.1.1 - Características Importantes do MGEN	48
3.2 - ACTERNA EXAMINE DA3600 - DATA NETWORK ANALYZER.....	52
3.2.1 - Características principais do Acterna.....	53
3.2.2 - Identificar e medir a qualidade de serviço (QoS).....	53
3.2.3 - Os benefícios do Acterna	54
3.2.4 - Roteamento em tempo real e sinalização dos protocolos de monitoramento.....	54
3.2.5 - Estatísticas de fluxo em tempo real em Acterna	54
3.2.6 - Transmissão em Acterna	55
4 - CAPÍTULO IV: ESPECIFICAÇÃO DOS TESTES E, CENÁRIO DE TESTE.	56
4.1 - Especificação dos Testes Laboratoriais:	56
4.1.1 - O que testar e quais testes fazer	57
4.2 - Cenário dos testes de medições.....	61
4.2.1 - Os equipamentos de comutação presentes no laboratório.....	62
4.2.2 - Readaptação da topologia física em lógica	65
5 - CAPÍTULO V: RESULTADOS PARCIAIS - MEDIÇÕES LABORATORIAIS.	70
5.1 - Objetivos das medições parciais sobre a viabilidade dos codecs em relação aos equipamentos de diferentes plataformas.....	70
5.1.1 - Porquê realizar estes testes.....	71
5.1.2 - Critérios metodológicos para desenvolvimento desses testes	71
5.1.3 - Resultado - Matriz – correlacionando codecs e os equipamentos de testes.....	72
5.1.4 - Interpretação dos resultados parciais dos testes de CODEC	73
5.2 - Testes preliminares sobre a QoS e LFI	73
5.2.1 - Porquê realizar esses testes.	74
5.2.2 - Metodologia genérica do cenário de desenvolvimento das medições parciais dos testes de LFI com QoS e análise dos protocolos.	74

5.3	Testes adicionais usando gerador acterna e ramais telefônicos sem QoS/LFI.....	77
5.4	- Testes Medições com fragmentação usando acterna medição sem QoS e LFI habilitado nas interfaces e usando ramais telefônicos para conversa interativa.....	78
5.4.1	- Resultado da comparação do desempenho da rede com e sem QoS/LFI - MGEN. 81	
5.5	- TESTES DE FRAGMENTAÇÃO USANDO ACTERNA MEDIÇÃO COM QoS E LFI.....	85
5.5.1	- Interpretação V - Dos resultados dessas medições.....	88
5.6	- QUANTO AOS TESTES DE COMPRESSAO DE CABEÇALHO RTP.....	90
5.6.1	- Porquê realizar esse teste.....	91
5.6.2	- Metodologias das medições dos testes de compressão de cabeçalho RTP.....	91
5.6.3	- Resumo dos resultados de teste sem compressão.....	92
5.7	- Resumo do resultado dos testes, mas habilitando a compressão.....	93
5.7.1	- Matriz relacionando parâmetros da rede com modelagem com/sem cRTP.....	93
5.7.2	- Interpretação dos Resultados parciais da compressão de cabeçalho RTP.....	94
5.8	- Compressão com telas dos pacotes capturados no backbone IP/MPLS.....	95
5.9	- Resultados de testes pré-liminares sobre as medições de CODECs, LFI, cRTP, comportamento da rede, e ocupação da banda por aplicações.....	95
5.9.1	Quanto aos CODECs testados:.....	96
5.9.2	- Quanto aos testes de compressão:.....	96
5.9.3	- Quanto aos testes de fragmentação com intercalação:.....	97
6	- CAPÍTULO VI: MEDIÇÕES COMPLEMENTARES COM TRÁFEGOS DE DIFERENTES CODECS.....	99
6.1	- Objetivo das medições correlacionando LFI, QoS, cRTP e CODECs em um mesmo tráfego.....	99
6.1.1	- Porquê estes testes.....	100
6.1.2	- Metodologia de desenvolvimento dos testes.....	100
6.1.3	- Caracterização de perfil de tráfegos nas medições sem QoS, sem LFI, sem cRTP, com os Codecs g729,g726,g711.....	100
6.1.4	- Caracterização do perfil de tráfegos nas medições com LFI habilitado a 640bytes de fragmento, com QoS, com cRTP desabilitado e usando os codecs g711,g726,g729.....	106
6.1.5	- Caracterização de perfis de tráfegos nas medição com QoS, com cRTP, LFI habilitado, usando o codec g729, com dois fluxos ftp concorrentes.....	112
6.1.6	- Caracterização de perfil de tráfegos nas medição com QoS negociada, com cRTP, com LFI, usando os codec de voz g729,g726,g729 associado a um fluxo FTP. 116	
7	- CAPÍTULO VII – RESULTADOS COMPLEMENTARES - TESTES E MEDIÇÕES ..	124
7.1	- Resultados Finais.....	124
7.1.1	Matriz de resultados.....	124
7.1.2	- Análise a nível do domínio backbone IP/MPLS.....	132
7.1.3	- Síntese dos resultados.....	134
7.1.4	- Matriz de percentual de ocupação da banda por cada teste.....	138
7.1.5	- Recomendações de boas práticas.....	139
8	- CAPÍTULO VIII – CONCLUSÃO DA DISSERTAÇÃO E ESTUDOS FUTUROS.....	141
8.1	- Conclusão técnica.....	141
8.2	- Conclusão do estudo dissertativo.....	142
8.3	- Estudos futuros:.....	146
9	- CAPÍTULO IX – REFERÊNCIAS BIBLIOGRÁFICAS & REFERÊNCIAS CONSULTADAS.....	147
9.1	- REFERÊNCIAS BIBLIOGRÁFICAS.....	147
9.2	- REFERÊNCIAS CONSULTADAS.....	150

10	- CAPÍTULO X – APÊNDICE I.....	156
10.1	- Outros Resultados parciais da compressão de cabeçalho RTP	156
10.1.1	Teste com 1 fluxo com e sem compressão	156
10.1.2	- Análise em backbone.....	158
10.1.3	- Pacote RTCP capturado no teste com dois fluxos comprimidos	164
10.2	- MGEN DETALHAMENTOS ADICIONAIS	164
10.2.1	- Script MGEN - Controle e Moldagem de Tráfego em FRF.12 – sem QoS garantida.165	
10.3	- ACTERNA	167
10.3.1	Detalhes a nível dos protocolos e QoS apresentados com saída do Acterna....	167
10.3.2	Tela ilustrativa da Medição Sem QoS e Sem LFI G726 e Sem cRTP	173
11	- CAPÍTULO XI – ANEXOS.....	176
11.1	- ESTUDOS CONCEITUAIS SOBRE IP VPN/MPLS.....	176
11.2	- TECNOLOGIA MPLS (Multiprotocol Label Switching)	176
11.2.1	- Algumas considerações importantes sobre as redes MPLS	177
11.2.2	- Terminologia MPLS.....	179
11.2.3	- Label – (Etiqueta ou Rótulo).....	180
11.2.4	- MPLS – e os mecanismos de encaminhamento dos pacotes.	183
11.2.5	- MPLS e o seu nível de agregação dos fluxos.....	184
11.2.6	- De entre algumas vantagens tecnológicas, constam:.....	185
11.2.7	- Funcionamento e transporte de dados MPLS sobre os nós de acesso....	187
11.3	- VPN / MPLS.....	188
11.3.1	- Benefícios da VPN/MPLS para os serviços e fornecedores.	189
11.3.2	- VPN - visão do cliente da rede	190
11.3.3	- VPN – PE's a visão do provedor de serviços da rede	191
11.3.4	- VPNs MPLS e as tabelas de encaminhamento (VRFs).....	192
11.4	- Protocolo IP e os princípios de serviços em redes IP.....	194
11.4.1	- Formato do Datagrama IP	196
11.4.2	- Fragmentação e remontagem de pacotes a nível IP.	198
11.4.3	- Remontagem de pacotes fragmentados	203
11.4.4	- Princípio do algoritmo de remontagem de pacotes	204
12	- CAPÍTULO XII - CONTEXTUALIZAÇÃO TEÓRICA - CODECS, RTP e cRTP.....	208
12.1	- CODECS	208
12.1.1	- FILOSOFIA DOS CODEC's USADOS NOS TESTES	209
12.2	- Protocolo RTP (Real Time Protocol) e a sua compressão	212
12.2.1	- Descrição dos campos do cabeçalho RTP [84],[89]	214
12.2.2	- RTP Compressão de cabeçalho	215
13	- CAPÍTULO XIII – CONSIDERAÇÕES SOBRE QoS.....	219
13.1	- Qualidade de Serviço (QoS) – Quality Of Service.....	219
13.1.1	- Visão Geral de QoS.....	220
13.1.2	- Parâmetros que influenciam no planeamento de QoS.....	221
13.1.3	- Alocação de Recursos	225
13.2	- Especificação da implementação de CoS - filas de QoS em roteadores Cisco	230
13.2.1	- Do mapeamento de Classes de Serviços (CoS):.....	231
13.2.2	- Implementação e verificação de AutoQoS.....	234
13.2.3	- Definindo políticas para cada classe de tráfego.	236
13.2.4	- Disciplinas de Escalonamento para Optimização de Desempenho.	237

ÍNDICE DE LISTA DE FIGURAS

Figura 1 - Frame Relay - Topologia Típica [24]	28
Figura 2 - Cabeçalho de Frame Relay de 2 bytes [30]	30
Figura 3: Generic Traffic Shaping [12].	36
Figura 4 - Committed Access Rate com token bucket [13].....	37
Figura 5 - Fragmentação e intercalação - readaptado [20].	43
Figura 6 - Processo de enfileiramento dos pacotes na interface FRF.12 e LFI [1]	44
Figura 7 - Atraso de serialização dos pacotes em um link de 64kbps (Readaptado)[20]. ...	45
Figura 8 - Script Exemplo - MGEN (Trafego01_a_CPE02).....	49
Figura 9 - Topologia Física – Inicial.	61
Figura 10 - Topologia lógica UFF – OP-Operadora de Telecomunicações	67
Figura 11 - Cenário de Implementação teste análise de CODECs [37]	72
Figura 12 - Fragmentação com LFI e QoS	75
Figura 13 - dos testes sem QoS e sem LFI habilitado usando o G729 e sem cRTP.....	79
Figura 14 - Script MGEN - Controle e Moldagem de Tráfego em FRF.12.	82
Figura 15 - Resultado a partir do MGEN para testes sem QoS	84
Figura 16 - Aplicação de LFI a rede de pacotes com frame de voz simulado pelo MGEN	86
Figura 17 - Aplicação de LFI e QoS a redes de pacotes priorizando os quadros de voz. ...	87
Figura 18 - Pacotes sem compressão capturados no acesso FR de 512K.....	92
Figura 19 - Pacotes Comprimidos capturados no acesso FR de 512K.....	94
Figura 20- Medição Sem QoS e Sem LFI G729 e Sem cRTP	103
Figura 21 - Medição Sem QoS e Sem LFI G726 e Sem cRTP	104
Figura 22 - Medição Sem QoS e Sem LFI G711 e Sem cRTP	105
Figura 23 - Gráfico de Jitter dos testes Sem políticas QoS, Sem cRTP, sem LFI, testados com Três codecs diferentes.....	106
Figura 24 - Medição Com QoS e Com LFI G729 e Sem cRTP	109
Figura 25 - Medição Com QoS e Com LFI G726 e Sem cRTP	110
Figura 26 - Medição Com QoS e Com LFI G711 e Sem cRTP	111
Figura 27 – Gráfico de representação de variação do atraso para testes Com políticas QoS, Sem cRTP, com LFI-640bytes, testados com Três codecs diferentes.....	111
Figura 28 Medição de Jitter para testes Com políticas QoS, com cRTP, com LFI- 540bytes, testados com codecs G729 e dois tráfegos FTP e um fluxo de voz.	115
Figura 29 - Gráfico de representação de variação do atraso para testes Com políticas QoS, com cRTP, com LFI-540bytes, testados com codecs G729 e dois tráfegos FTP e um fluxo de voz.....	115
Figura 30 - Medição Com QoS e Com LFI_540_G729 e Com cRTP	120
Figura 31 - Medição Com QoS e Com LFI_540_G726 e Com cRTP	121
Figura 32 - Medição Com QoS e Com LFI_540_G711 e Com cRTP	121
Figura 33 - Gráfico comparativo da medição Jitter dos testes de um fluxo de voz com dois tráfegos ftp e, medição de QoS usando três codecs diferentes.....	122
Figura 34 - Detalhamento adicionais sobre pacotes sem compressão capturados no acesso FR de 512K.....	156
Figura 35 - Detalhamento adicionais sobre Pacotes Comprimidos capturados no acesso FR de 512K.....	157
Figura 36 - Pacote sem compressão no Backbone IP/MPLS	158
Figura 37 - Informações do Frame capturados no acesso Backbone - MPLS.....	159
Figura 38 - Pacote Ethernet - análise a partir de backbone IP / MPLS	160
Figura 39 -Pacote MPLS	160
Figura 40 - Pacote IP	161
Figura 41 - Pacote UDP	161
Figura 42 - Pacote RTP	162

Figura 43 - Testes com dois fluxos de voz no backbone IP/MPLS.....	163
Figura 44 - Pacotes RTCP capturados no backbone IP/MPLS	164
Figura 45 – Detalhamento adicionais sobre o Script MGEN - Controle e Moldagem de Tráfego em FRF.12.....	165
Figura 46 - Detalhamento adicionais sobre o Controle e Moldagem de Tráfego em Frame Relay – “QoS não garantida”	166
Figura 47 - Aplicação de LFI a rede de pacotes com frame de voz - simulado pelo MGEN	167
Figura 48 - Detalhamento adicionais da Fragmentação Interleaving com QoS e LFI	168
Figura 49 - Detalhes do fluxo de Voz_1 de 2 a nível de protocolos Frame relay e IP.....	169
Figura 50 - Detalhes do fluxo de Voz_2 de 2 a nível de protocolos IP e UDP	170
Figura 51 - Detalhes do fluxo classe business_1 de 2 tamanho do fragmento e nº sequência.	170
Figura 52 - Detalhes do fluxo classe business_1 de 2 a nível de protocolos IP e UDP. ...	171
Figura 53 -Fragmento 2 da classe business	172
Figura 54 - Detalhamentos adicionais sobre a Medição Sem QoS e Sem LFI G729 e Sem cRTP	173
Figura 55 - Trecho ilustrando parâmetros de QoS para dados em Tráfego híbrido Sem QoS	175
Figura 56- Formato do Label MPLS [61].....	180
Figura 57 - Posição do cabeçalho MPLS no envio de segmento TCP com IP, PPP	181
Figura 58 - Enfileiramento de cabeçalhos MPLS em um pacote de dados [85]	182
Figura 59 - VPN - visão do cliente da Rede [87]	191
Figura 60 - VPN visão do provedor de serviços da rede [87]	191
Figura 61 - VRF's de sites com múltiplas VPN em um core MPLS [87]	193
Figura 62 - Formato do cabeçalho IP (Figura readaptada) [7]	197
Figura 63 - Fragmentação e remontagem em uma rede de mesmo tamanho de MTU [8].....	199
Figura 64 - Fragmentação e remontagem em uma rede de MTU diferentes	201
Figura 65 - Separação de tráfego RTP para compressão de cabeçalho [98].	216
Figura 66 - Arquitetura funcional do <i>DiffServ</i> [51]	227
Figura 67 - Escalonamento FIFO [53].....	239
Figura 68 - Técnica enfileiramento PQ [53].....	240
Figura 69 - Técnica de Enfileiramento Justo (FQ) [53].	242
Figura 70 - Disciplina WFQ (Weighted fair queuing)	243
Figura 71 - Disciplina WRR (<i>Weighted Round Robin</i>) [53].	244
Figura 72 - Funcionamento do Algoritmo Deficit Weighted Round Robin [53]	246

ÍNDICE DE LISTA DAS TABELAS

Tabela 1 - Delay de pacotização por tamanho de <i>payload</i> [3]	45
Tabela 2 - Cálculo do tamanho do fragmento [20].....	46
Tabela 3- Demonstração do cálculo do Tamanho máximo de MTU de enlace	46
Tabela 4 – Tempo de retardo de bloqueio dos pacotes por banda disponível (readaptada) [15].....	47
Tabela 5 - Exemplo de classificação de tráfego a partir do script MGEN.	51
Tabela 6 - Definições de classes e modelagem FRTS configurado nos roteadores CPE da OP	68
Tabela 7 - Porcentagem de tolerância a perda de pacotes por codecs de voz [37].....	73
Tabela 8 - Fragmentação com e sem LFI e QoS	81
Tabela 9 - Compressão de Cabeçalho e não compressão de cabeçalho	93
Tabela 10 - Caracterização dos Perfis de QoS dos Tráfegos nos CPE's (Sem políticas QoS, Sem cRTP, sem LFI, testados com Três codecs diferentes).....	101
Tabela 11 - Medição da banda Sem QoS, Sem cRTP, sem LFI, codec G729.....	102
Tabela 12 - Valores de Jitter dos testes Sem políticas QoS, Sem cRTP, sem LFI, testados com Três codecs diferentes.....	103
Tabela 13 - Caracterização dos Perfis de QoS dos Tráfegos nos CPE's (Com políticas QoS, Sem cRTP, com LFI-640bytes, testados com Três codecs diferentes)	107
Tabela 14 - Banda ocupada na medição com QoS, Sem cRTP, com LFI-540bytes, G729	108
Tabela 15 - Valores de Jitter de testes Com políticas QoS, Sem cRTP, com LFI-640bytes, testados com Três codecs diferentes.....	108
Tabela 16 - Caracterização dos Perfis de QoS dos Tráfegos nos CPE's (1 Fluxo real time (Voz) e 2 tráfegos Ftp concorrentes)	113
Tabela 17 - Ocupação da Banda para testes Com políticas QoS, com cRTP, com LFI-540bytes, testados com codecs G729 e dois tráfegos FTP e um fluxo de voz.	113
Tabela 18 - Valores de Jitter para testes Com políticas QoS, com cRTP, com LFI-540bytes, testados com codecs G729 e dois tráfegos FTP e um fluxo de voz.....	114
Tabela 19 - Caracterização dos Perfis de QoS dos Tráfegos nos CPE's (Com políticas QoS, Com cRTP, com LFI-540bytes, testados com Três codecs diferentes	116
Tabela 20 - Ocupação da Banda para testes Com políticas QoS, com cRTP, com LFI, testados com codecs G729 um fluxo de voz e um tráfego FTP.	117
Tabela 21 - Ocupação da Banda para testes Com políticas QoS, com cRTP, com LFI-540bytes, testados com codecs G726 um fluxo de voz e um tráfego FTP	118
Tabela 22 - Ocupação da Banda para testes Com políticas QoS, com cRTP, com LFI-540bytes, testados com codecs G711 um fluxo de voz e um tráfego FTP	118
Tabela 23 - Valores de Jitter para testes Com políticas QoS, com cRTP, com LFI-540bytes, testados com um tráfego de voz usando os codecs G729, G711 e G726 e um tráfego FTP.	119
Tabela 24- Matriz dos Resultados de medidas de QoS, RTP e LFI usando os codecs G711/G726/G729	125
Tabela 25 - Análise a partir do Backbone MPLS	133
Tabela 26 - Quantidades de canais VoIP usando G729 com LFI e cRTP.....	135
Tabela 27 - Quantidade de canais considerando QoS, LFI e cRTP habilitados sem dados	135
Tabela 28 - Quantidades de canais em tráfegos VoIP sem QoS e sem cRTP usando G729	135
Tabela 29 - Quantidades de canais VoIP em enlace 512kbps, LFI-640bytes, G711 e cRTP	136

Tabela 30 - Quantidades de canais VoIP em enlace 512kbps, LFI -540bytes, G729 sem cRTP	136
Tabela 31 - Quantidades de canais VoIP em enlace 512kbps, LFI-640bytes, G729 e cRTP	136
Tabela 32 - Quantidades de canais VoIP em enlace 512kbps, LFI-640bytes, G726 e cRTP	137
Tabela 33 - Quantidade de canais de VoIP em enlace 512kbps sem cRTP, com QoS e G729	137
Tabela 34 - Quantidade de canais de VoIP em enlace 512kbps com cRTP, com QoS e G729	138
Tabela 35 - Matriz de percentual de ocupação da banda por cada teste.....	138
Tabela 36 - Matriz Quantidade de canais banda disponível para VoIP.....	141
Tabela 37 - Medição de Compressão com cRTP desabilitado.	157
Tabela 38 - Medição de compressão com cRTP habilitado.	158
Tabela 39 - Tamanho da banda ocupada em medição com dois pares de ramais telefônicos.	163
Tabela 40 - Ocupação da Banda da medição Sem QoS, Sem cRTP, sem LFI, codec G729.	174
Tabela 41 - Fragmentação quadro Ethernet [7].	202
Tabela 42 - Cálculos de Banda em enlace FRF12 de acordo com os Codecs [5],[3].....	210
Tabela 43 - Atraso de formação de quadro em G723[5]	211
Tabela 44 - Formato de cabeçalho RTP [84].....	213
Tabela 45 - RTP Compressão de cabeçalho [5]	216
Para os testes de cRTP foram levados em conta a contagem do valor numérico do cabeçalho de alguns protocolos. Abaixo segue a demonstração do cálculo, com base na Tabela 46 acima - Cálculos de Banda em enlace FRF12 de acordo com os Codecs” [3]:	
Tabela 46 - Cálculos de Banda em enlace FRF12 de acordo com os Codecs” [3]:	217
Tabela 47 - Vazão para diversas aplicações [51]	222
Tabela 48 – Sensibilidade para diversas aplicações [52]	224
Tabela 49- Definições das CoS suportadas pelos equipamentos comutação Cisco [27]...	231
Tabela 50 - Classes de tráfego definidas pela AutoQoS [27].....	232
Tabela 51 – Filas-Classes AF PHB - DSCP, probabilidade de descarte de pacotes [27]..	233
Tabela 52 - Funções <i>DiffServ</i> - recursos da Cisco para habilitar a AutoQoS [27].	235
Tabela 53 - Definição de políticas de QoS para as Classes de Tráfego de serviços [27].	236

LISTA DAS ABREVIATURAS

- **ACELP:** *Algebraic Code Excited Linear Prediction*
- **ADSL:** *Asymmetric Digital Subscriber Line*
- **AF:** *Assured Forward*
- **ANSI:** *American National Standard Institute*
- **AQ:** *Assured Queue*
- **AR:** *Access Rate*
- **ARPANET:** *Advanced Research Projects Agency Network*
- **AS:** *Sistemas Autônomos*
- **ATA:** *Analogic Telephone Adapter*
- **ATM:** *Asynchronous Transfer Mode*
- **AToM:** *Any Transport over MPLS*
- **BA:** *Behavior Aggregate*
- **BB:** *Bandwidth Broker*
- **Bc:** *Committed burst size*
- **Be** - *Excess burst size*
- **BECN:** *Backward Explicit Congestion Notification*
- **BGP:** *Border Gateway Protocol*
- **CAR:** *Committed Access Rate*
- **CBQ:** *Class-based Queuing*
- **CBR:** *Constant Bit Rate*
- **CBWFQ:** *Class-based weighted fair queueing*
- **CIR:** *Committed Information Rate*
- **CNG:** *Confort Noise Generator*
- **CoS:** *Class of Service;*
- **CPE:** *Customer Premise Equipment*
- **CRT:** *Centro de referência Tecnológica*
- **cRTP:** *Compress Real Time Protocol*
- **CSC:** *Class Selector Compliant*
- **CSRC:** *Contributing source Count*
- **DARPA:** *Defense Advanced Research Projects Agency*
- **DCE:** *Data Communications Equipment*
- **DTX:** *Discontinuous Transmission*
- **DE:** *Discard Eligibility*
- **DECnet:** *Digital Equipment Corporation network protocols*
- **DiffServ:** *Differentiated Services*
- **DLCI:** *Data-Link Connection Identifier*
- **DoS:** *Denial-of-service*
- **DSCP:** *Diffserv Code-Point*
- **DSP:** *Digital Signal Processor*
- **DTE:** *Data Terminal Equipment*
- **DWRR:** *Deficit Weighted Round Robin*
- **ECP:** *Encryption Control Protocol*
- **EF:** *Express Forward*
- **EoMPLS:** *Ethernet over MPLS*
- **FCFS:** *First Come First Served*
- **FCS:** *Frame Check Sequence*
- **FDDI:** *Fiber Distributed Data Interface*
- **FECN:** *Forward Explicit Congestion Notification*
- **FECs:** *Forwarding Equivalence Class*

-
- **FIFO:** *First In First Out*
 - **FIRJAN** – *Federacao das Industrias do Estado do Rio de Janeiro*
 - **FQ:** *Fair Queuing*
 - **FR:** *Frame Relay*
 - **FRAD:** *Frame Relay Access Device*
 - **FRF.12:** *Fame Relay Fórum v12*
 - **FRTS:** *Frame Relay Traffic Shaping*
 - **FS:** *Full Status*
 - **FTP:** *File Transfer Protocol*
 - **FXO:** *Foreign eXchange Office*
 - **FXS:** *Foreign eXchange Subscriber*
 - **GPS:** *Global Positioning System*
 - **GSM:** *Global System for Mobile Communications*
 - **GSMEFR:** *GSM Enhanced Full Rate*
 - **GTS:** *Generic Traffic Shaping*
 - **HDLC:** *High-LevelData Llink Control*
 - **HTTP:** *Hyper Text Transfer Protocol*
 - **ICMP:** *Internet Control Message Protocol*
 - **ICPIF:** *Calculated Planning Impairment Factor*
 - **ID:** *Identification*
 - **IETF:** *Internet Engineering Task Force*
 - **IMS:** *IP Multimedia Subsystem*
 - **IP:** *Internet Protocol;*
 - **IPTV:** *Internet Protocol Television*
 - **IPv6:** *Internet Protocol version 6*
 - **IPX:** *Internetwork Packet Exchange*
 - **ISDN:** *Integrated Services Digital Network*
 - **IS-IS:** *Intermediate System to Intermediate System Routing Exchange Protocol*
 - **ITU:** *International Telecommunication Union*
 - **ITU-T:** *Telecommunication Standardization Sector*
 - **Kbps:** *kilobits per second*
 - **LAN:** *Local area network*
 - **LAPD:** *Link Access Protocol on the D-channel*
 - **LBS:** *Label Based Switching*
 - **LCD:** *Liquid Crystal Display*
 - **LDP:** *Label Distribution Protocol*
 - **LER:** *Label Edge Router*
 - **LFI:** *Link Fragmentation and Interleaving*
 - **LLQ:** *Low-latency queuing*
 - **LOP:** *Laboratório de Operadora de Telecomunicacoes*
 - **LSP:** *Label Switch Path*
 - **LSRs:** *Label Switch Router*
 - **MAC Address:** *Media Access Control*
 - **MF:** *Multi-field*
 - **MGEN:** *MultiGenerator*
 - **MIPS:** *Million Instructions Per Second*
 - **MLPP:** *Multilink point-to-point protocol*
 - **BGP-MP:** *Border Gateway Protocol - Multiprotocol*
 - **MPLS:** *Multiprotocol Label Switching*
 - **MP-MLQ:** *Multi Pulse-Maximum Likelihood Quantization*
 - **MPPP:** *Multilink PPP*

-
- **MTTR:** *Mean Time To Repair*
 - **MTTU:** *Mean Time To Understand*
 - **MTU:** *Maximum Transmission Unit*
 - **NNI:** *Network-Network Interface*
 - **NTP:** *Network Time Protocol*
 - **OP:** *Operadora de Telecomunicacoes*
 - **OS:** *Operating Systems*
 - **OSPF:** *Open Shortest Path First*
 - **PABX (PBX):** *Private Automatic Branch eXchange*
 - **PCM:** *Pulse Code Modulation*
 - **PE:** *Premise Equipment*
 - **PHB:** *Per Hop Behavior*
 - **PoPs:** *Points of Presence*
 - **PPP:** *Point-to-Point Protocol*
 - **PPS:** *packets per second*
 - **PQ:** *Priority Queuing*
 - **PT:** *Payload Type*
 - **PVC:** *Permanent Virtual Circuit*
 - **QoS:** *Quality of Service*
 - **RIP:** *Routing Information Protocol*
 - **ROT:** *Router*
 - **RR:** *Round Robin*
 - **RSVP:** *Resource Reservation Protocol*
 - **RTCP:** *Real Time Control Protocol*
 - **RTP:** *Real Time Protocol*
 - **SAA:** *Service Assurance Agent*
 - **SDUs:** *Service Data Unit*
 - **SE:** *Status Enquiry*
 - **SLA:** *Service Level Agreement*
 - **SONET:** *Synchronous Optical Network*
 - **SDH:** *Synchronous Digital Hierarchy*
 - **SSRC:** *Synchronization source*
 - **STM:** *Synchronous Transport Module*
 - **TCP:** *Transmission Control Protocol*
 - **TE:** *Traffic Engineering*
 - **TOS:** *Type of Service*
 - **TTL:** *Time to Live*
 - **UDP:** *User Datagram Protocol*
 - **UFF:** *Universidade Federal Fluminense*
 - **UNI:** *User to Network Interface*
 - **VAD:** *Voice Activity Detector*
 - **VLANs:** *Virtual Local Area Network*
 - **VoATM:** *Voice Over ATM*
 - **VoIP:** *Voice over Internet Protocol*
 - **VPLS:** *Virtual Private LAN Services*
 - **VPN:** *Virtual Private Network*
 - **VRF:** *Virtual Routing and Forwarding*
 - **WAN:** *Wide Area Network*
 - **WFQ:** *Weighted Fair Queuing*
 - **WRED:** *Weighted Random Early Detection*
 - **WRR:** *Weighted Round Robin*

RESUMO

Esta dissertação descreve os resultados das medições observadas em um dos Laboratórios de uma Operadora de Telecomunicações (LOP), onde foram avaliados e analisados alguns requisitos de QoS em redes de pacotes IP (*Internet Protocol*). Essas medições foram feitas no âmbito do objetivo desta dissertação que é avaliar formas de prover serviços VoIP (*Voice over Internet Protocol*) em redes de pacotes conforme a recomendação do padrão FRF.12. Essa rede é assim, uma rede de link de 512kbps que também provê serviços VoIP compartilhados, concorrentemente com dados e serviços multimídia. Dos itens analisados destacam-se: Análise de Codecs; QoS (*Quality Of Service*) *Diffserv*; Compressão de cabeçalho RTP (*Real Time Protocol*) - cRTP; Fragmentação com intercalação - LFI; Comportamento da Rede em situações diversas; a adequação do software *free Multi Generator* (MGEN) de geração - medição - coleta de dados, em redes. A análise foi, essencialmente, em enlace Frame Relay nos CPE (*Customer Premise Equipment*), passando pelo *Backbone IP VPN / MPLS Multicast*, pois o Frame Relay Fórum v12 (FRF.12) dá suporte à intercalação de voz entre os pacotes de dados. O FRF.12 é indispensável, pois esta dissertação tem como objetivo realizar um conjunto de testes e medidas que avaliam a aplicação dos serviços VoIP em links de baixa capacidades com tráfego de dados compartilhados. Para oferecer esse serviço e de qualidade é necessário fragmentar e intercalar frames de voz entre os pacotes de dados usando o FRF.12. Depois do estudo teórico das recomendações, normas de padronização internacional e dos fabricantes, foram realizados testes que resultam na validação prática de toda a teoria outrora analisada através de testes específicos que comprovam em definitivo a viabilidade das aplicações VoIP em uma rede de enlace de baixa velocidade. Feitos esses testes chegou-se a conclusão de que em determinados casos não se revela necessário nem preocupante o aumento da banda para se puder prover determinados serviços. Na sequência dos testes foram também avaliados o desempenho, a ocupação da banda e a eficácia dos equipamentos - softwares. Da bancada dos testes e medições, provou-se o seguinte: que de fato consegue-se melhor otimização da banda ao realizar compressão do cabeçalho cRTP; que de fato a fragmentação de pacote FTP (*File Transfer Protocol*) com intercalação de pacotes VoIP faz reduzir o delay e *jitter*¹ para as aplicações de tempo real; que de fato a habilitação de QoS *Intserv* provê classificação e faz diferenciação dos tráfegos, e que o CODEC G729 apresenta melhor adequação em lidar com aplicações VoIP em routers² CISCO, disponível em CRT (Centro de referência Tecnológica) de uma LOP.

Palavras chaves: Qualidade de Serviço, VoIP, Avaliação de desempenho.

¹ **Jitter** - Variação de atraso na transmissão de pacotes

² **Routers** - Dispositivos de rede utilizados em comutação

ABSTRACT

This thesis describes the results of the measurements observed in the Telecom Operator Laboratory (LOP), where some QoS in packet networks IP (Internet Protocol) were evaluated and analyzed. These measurements were made as suggests the objective of this thesis - to evaluate ways to provide VoIP (Voice over Internet Protocol) packet networks as recommended by the standard FRF.12. This network is a 512kbps bandwidth that also provides VoIP services shared concurrently with data and multimedia services. Of the items examined include: Analysis of codec's, QoS (Quality Of Service) Diffserv, RTP header compression (Real Time Protocol) - cRTP; Link Fragmentation and Interleaving (LFI); network behavior in different situations, the adequacy of free software MultiGenerator (MGEN) generation - measurement - data collection networks. The analysis was therefore mainly on the link Frame Relay CPE (Customer Premise Equipment), through the backbone IP VPN / MPLS multicast because the Frame Relay Forum v12, supports voice intercalation between data packets. The FRF.12 it's indispensable, therefore this thesis has as objective to carry through a set of tests and measures that evaluate the application of the VoIP services in links of low capacities with traffic of shared data. To offer this service and of quality it is necessary to execute LFI of voice frames enters the packages of data using the FRF.12. After the theoretical study of the recommendations, international regulation standards and those of the manufacturers, validation tests have been conducted that result in practice, all the theory previously analyzed by specific tests that definitively prove the viability of VoIP applications in a network of low-speed link. This has made these tests come to the conclusion that in certain cases it is not necessary to alarmingly increase bandwidth in order to provide certain services. In the test sequence, the evaluations were performed, the bandwidth occupation, and effectiveness of equipment and software. Bench tests and measurements proved that in fact bandwidth optimization can be better when performing header compression - cRTP; and for a fact packet fragmentation FTP (File Transfer Protocol) and VoIP packet interleaving reduce the delay and jitter for real time applications, which in fact enables IntServ QoS provide classification and differentiation of traffic, and that the G729 CODEC has better suitability in dealing with Cisco routers in VoIP applications, available in CRT (Centre for Technological Reference) of a LOP.

*Keywords: **Quality of Service, VoIP, Performance Assessment***

1 - *CAPÍTULO I: INTRODUTÓRIO*

*“Atribua 'a' outra pessoa um bom conceito,
com a qual ela possa viver”*
- Dale Carnegie

“O mundo abre passagem para qualquer um que saiba onde está indo”
- David Starr Jordan

1.1 - **Introdução**

Foram realizadas no CRT - *Centro de Referência Tecnológica* - de uma OP (Operadora de Telecomunicações) através do convênio de Cooperação Técnica de 02/2003 estabelecido entre as partes - Departamento de Eng. Telecomunicações da UFF (*Universidade Federal Fluminense*) e a referida OP- um conjunto de testes a fim de avaliar os serviços VoIP (*Voice over Internet Protocol*) em links de baixa capacidade - 512kbps com tráfego compartilhado de dados FTP³, conforme sugere o título dessa dissertação. Baseado neste objetivo, a avaliação dos testes práticos que são apresentados nos próximos capítulos, tem como principais itens medidos e analisados e os principais resultados obtidos dos seguintes itens pesquisados: Compressão⁴ de Cabeçalho RTP (cRTP); Análise de Codecs; Fragmentação com Intercalação de voz (LFI), e QoS (Qualidade de Serviço – *Quality of Service*). Esses quatro itens constituem mecanismos de melhoria de enlaces em redes com *déficit* de banda. Os itens em causa correlacionam-se de forma íntima e harmônica, uma vez que a rede operacional precisa de apresentar eficácia no que diz respeito às expectativas dos clientes, já que os clientes, em regra, pedem sempre um serviço “híbrido” a custo baixo e de boa qualidade. Sendo assim, o fornecedor precisa atender da melhor forma às exigências dos clientes, levando sempre em conta que vivemos em uma sociedade onde há fortes incidências de concorrência tecnológica e comercial. Desse modo, os fornecedores precisam lidar, de forma eficiente, com os seus recursos de telecomunicações a fim de garantir-lhes uma boa preferência.

³ **FTP:** Neste trabalho não se refere ao tipo de protocolo de transferência de arquivos, mas sim ao tipo de dados de sistema de arquivos.

⁴ **Compressão de cabeçalho RTP:** Em todo este trabalho, a cRTP foi habilitada apenas para tráfegos de tempo real como a Classe de Serviço - Voz, não em todas as Classes de Serviços.

De entre os recursos infra-estruturais, uma das situações a lidar é a questão de banda. A banda passante e a banda a ser alocada e disponibilizada aos clientes, tem sido um recurso escasso e que merece um bom gerenciamento, principalmente quando se usa *links*⁵ de baixa capacidade comportando tráfegos híbridos. Uma das soluções até hoje abraçada é a implementação rigorosa dos quatro itens anteriormente descritos ao invés de aumentar sempre a banda, o que implica altos investimentos financeiros e, em contrapartida, poucos clientes contratam serviços que demandam muita banda.

No referido Laboratório de Operadora de Telecomunicações (LOP), esses experimentos foram testados em um ambiente com roteadores CISCO passando pelo *Backbone*⁶ IP/MPLS multifornecedor de um dos LOP concebido para tal fim, conforme a parceria de trabalho vigente na época com a UFF. Os roteadores foram, portanto, essencialmente do fabricante Cisco das séries 2600/1751v/1760 (disponível pela operadora) denominados equipamentos CPE (*Customer Premise Equipment*), usados em enlace de baixa velocidade (512kbps) usando protocolos de nível-2 FRF.12 e MPPP no acesso através das interfaces V.35 e G703. Durante as bancadas de testes, foram também usados equipamentos de outros fabricantes como HP3800,⁷ MXOne, (disponíveis na FIRJAN - *Federação das Indústrias do Estado do Rio de Janeiro*) e vários softwares de geração e análise de tráfego como *Examine Acterna*, *MGEN*, *Asterisk*, *SmartWindows*, entre outros, permitindo assim que fosse analisado essencialmente os enlaces de acesso - Frame Relay nos CPE que provem link que trafegam dados que passam pelo *Backbone IP VPN / MPLS Multicast*.

MPLS, é a tecnologia de convergência multiplataforma para redes de banda larga – GigaRouters - atualmente usada em núcleos dos Backbones que acompanham as tendências das redes modernas atuais. Os experimentos citados foram assim realizados com o objetivo de avaliar e medir a eficiência dos serviços VoIP em redes de dados e, a adequação, interação dos equipamentos com relação a esses serviços, visando prover melhoria em serviços multimídia que a OP possa vir a oferecer para determinados clientes se assim os satisfizer, reaproveitando, dessa forma, as infra-estruturas

⁵ **Link:** Enlace ponto-a-ponto

⁶ **Backbone:** Corpo central da rede responsável por ligar redes menores.

⁷ Os equipamentos HP3800, MXOne e *Asterisk*, foram disponibilizadas pela FIRJAN, onde o colega Alex realizou testes de avaliação dos codec G729, G726, G723 e G711 usando estes equipamentos.

atualmente consideradas defasadas da realidade ou simplesmente incapazes de atender às demandas do mercado atual.

São testados os seguintes parâmetros que viabilizam uma boa prática de QoS:

- Delay; jitter; perda de pacotes; vazão; cabeçalho de pacotes; comportamento da rede em situação de estresse; ocupação da banda; classificação e policiamento dos pacotes; marcação de pacotes; verificação na íntegra da LFI⁸ (*Link Fragmentation and Interleaving*); cRTP (*Compression Real Time Protocol*) comparando o quanto muda na ocupação do enlace com a habilitação e a não habilitação da compressão; avaliação de CODEC - tolerância a perda e adequação às aplicações de tempo real; adequação dos tráfegos na rede, perfis de aplicações / tráfegos antes e depois de classificação, policiamento e conseqüentemente a viabilidade das aplicações VoIP incluindo repetidos testes com chamadas telefônicas reais entre os ramais configurados para tal propósito. Finalmente, vale também dizer que foram feitos outros testes complementares não relevantes para constar deste trabalho.

A realização das referidas medições foi possível graças aos convênios educacionais entre as instituições supracitadas, uma vez que foi de interesse da OP realizar esses conjuntos de bancadas de testes com diferentes soluções VoIP em redes de pacotes⁹ IP de link de baixa capacidade compartilhados com demais aplicações da rede do tipo FTP. Essas bancadas de testes propunham testar e provar a qualidade dos serviços multimídia sem ter que se preocupar em aumentar a largura da banda passante em uma rede multi-fornecedor e multiplataforma, ou preocupar-se em readaptar a infraestrutura física e em termos de softwares no cenário laboratorial da rede. O cenário laboratorial fora baseado no âmbito dos estudos da convergência CPE IP VPN através de backbone MPLS, e as recomendação Farne Relay Fórum v12 (FRF.12) nos roteadores de acesso.

Posto isso, um conjunto de testes dotados de técnicas de QoS (*DiffServ*) associadas aos mecanismos de melhoria de enlaces anteriormente mencionados, foi

⁸ **LFI** – Será o tamanho Máximo do fragmento de dados. Este tamanho Máximo representará a MTU de enlace.

⁹ **Pacotes**: São unidades de informações divididas normalmente em tamanhos (pacotes) definidos, e transmitidos aos poucos na rede de dados. O pacote representa uma unidade de dados que é roteada entre uma origem e um destino dentro de uma rede qualquer.

levado a cabo. Durante os testes, Softwares *free* MGEN também foram testados e aplicados em apoio aos testes. A associação e implementação das técnicas acima descritas, torna-se bastante útil quando se tem tráfego VoIP compartilhando, por exemplo, uma banda concorrentemente com grandes pacotes de dados FTP e outras aplicações multimídias como *stream de vídeo on demand*. A aplicação dessas técnicas em conjunto, permita com que se obtenha no atual cenário de testes de medições soluções de otimização que permitam aproveitar-se harmonicamente e de melhor forma da banda (estreita), reduzindo consideravelmente o retardo e a sua variação para as aplicações que trafegam na rede e dando suporte eficaz às aplicações de voz interativa, permitindo desse modo prover serviços VoIP de boa qualidade em uma rede de banda estreita compartilhada, conforme título desta dissertação.

Dado à aplicabilidade dos testes que se propõem serem realizados, afiguram-se como alguns dos objetivos, testar necessariamente a integração de diferentes soluções de QoS para VoIP e acesso em VPNs / MPLS através da convergência CPE IP VPN, tendo FRF.12 como tecnologia de acesso em enlace de 512kbps. Face ao exposto e como pressuposto, são testados parâmetros de “viabilidade” QoS, conforme anteriormente descritos.

São apresentados, necessariamente, resultados comprobatórios das medições de acordo com as recomendações das normas e padrões internacionais para aplicações de voz em rede de pacotes, pois nos dias de hoje, nota-se a crescente demanda dos serviços de telecomunicações pelos usuários finais que pedem cada vez mais banda para o comodismo próprio. Nessa ótica é também perceptível a crescente rede de serviços e aplicações que trafegam pela rede e cada uma delas demanda uma reserva de banda própria, pois cada aplicação é dotada de especificidade própria, por exemplo, no que concerne à sua tolerância a perda ou atraso bem como a variação do atraso. Percebe-se que as operadoras tendem a investir cada vez mais nos equipamentos mais modernos, (já que a tecnologia também assim proporciona) e migrar suas redes para acesso cada vez maior na questão de alocação quantitativa de banda passante, o que acarreta um alto custo e empreendimento.

É justo prover uma banda confiável e estável ao cliente de acordo com o seu consumo ou aquilo que contratou; é justo também que as operadoras controlem através

das políticas o uso dos links dos seus clientes finais através de políticas rígidas de QoS, evitando que o uso arbitrário de um cliente influencie negativamente na demanda operacional de um terceiro. Um bom caderno de testes de implementação de QoS, resulta-se em um bom serviço ainda que se considere um link de baixa velocidade levando-o a exaustão, onde pode ser alocado uma “infinitude” de usuários finais.

Práticas contrárias a uma política séria de QoS, não muito bem ajustadas, faria com que uma rede que tenha banda considerável, não deixasse de prover serviços de qualidade comprometida. Foi assim que a necessidade da OP serviu de base e motivação suficiente para a elaboração dessa dissertação, já que se tratava de um laboratório em um centro de referência tecnológica em telecomunicações. Por fim, convém ressaltar que as redes de telecomunicações nos dias de hoje, tiveram avanços consideráveis em termos de infra-estruturas físicas, lógicas e de tecnologia de redes (equipamentos de comunicação, comutação, etc). Entretanto, ainda a tecnologia IP continua sendo um adereço de utilização base na qual quase todas as tecnologias modernas de redes em termos de protocolos se sustentam. Uma análise atenta das características peculiares do protocolo IP, por exemplo, pode-se dizer que o IP é um protocolo de endereçamento de pacotes em redes IP, possuindo por si só várias limitações em lidar com os novos serviços de telecomunicações presentes no nosso dia-a-dia, visto que não foi projetado para lidar com determinadas aplicações cuja sensibilidade em termos de confirmação de entrega e facilidades de encaminhamento, requer garantias expressas.

Assim as redes IP lidam com pelo menos dois problemas bases nos dias atuais:

- 1 - A telefonia - as redes IP não lidam bem com as aplicações VoIP;
- 2 - As redes IP também lidam com problemas de tamanho máximo de dados que um link de segmento IP pode carregar – o tamanho da MTU. Em uma rede IP muitas vezes as informações são divididas em fragmentos menores para que possam ser transportadas de uma interface a outra. Entretanto, nem todas as informações podem ser quebradas, como é o caso dos conteúdos VoIP.

Dado as características das aplicações VoIP neste caso a técnica *Link Fragmentation and Interleaving* - LFI através da recomendação FRF.12 que permite

fragmentar e intercalar os *frames*¹⁰ de voz entre os pacotes FTP no nível de enlace, ajuda grandemente a resolver o problema. A fragmentação, no entanto, pode também ocorrer ao nível do IP, se por exemplo as informações a serem transportadas excederem o tamanho da MTU. No nível-2 (L2) também, pode ocorrer uma re-fragmentação dos dados FTP (anteriormente fragmentados no nível-3) com ou sem intercalação dos pacotes de voz usando os procedimentos p.ex. da fragmentação *Interleaving*, que é um procedimento “nativo” de nível-2(enlace), podendo ser implementado usando a tecnologia FRF.12 e MPPP.

Situando o problema em técnicas e formas de soluções, vale destacar que também a técnica como a cRTP, permite economizar a banda em média na ordem de 30%. Contudo, mostra-se necessária a escolha cuidadosa de CODECs que está associado ao cRTP que permite reduzir o volume da banda a ser consumida, permitindo assim agregar mais fluxos ao tráfego que poderiam ficar trafegando em média 25% de *overhead*¹¹ na rede. Assim em uma rede como a disponibilizada pela OP, viu-se oportuno a realização dos tais testes, conforme sugere a subsecção da estrutura da dissertação imediatamente a seguir.

1.1.1 - Estrutura da dissertação

Esta dissertação, para além do capítulo I - introdutório; tem como estrutura documental baseado no teor do seu objetivo mais doze (12) capítulos, a saber:

- ✓ Capítulo II - Neste capítulo serão também realizados estudos conceituais sobre tecnologia Frame Relay e as Recomendações Frame Relay Fórum v12 (FRF.12), fragmentação com intercalação a nível FRF.12 e Recomendações ITU-T (*International Telecommunication Union - Telecommunication Standardization Sector*);
- ✓ Capítulo III – Estudo e avaliação dos perfis do equipamento de teste *Acterna* e do *Software Free MGEN* e a sua contribuição para a operação na rede de teste

¹⁰ **Frame:** Unidade de informação que a Camada Interface de Rede utiliza para transmitir através do meio físico os dados recebidos da Camada de Rede.

¹¹ **Overhead :** São todas as informações dos protocolos usados para permitir que seus dados sejam transferidos de forma corretamente, podem ser informações de cabeçalhos de protocolos de transferências, protocolos de sinalização etc.

da OP e nos testes realizados nesta dissertação e, também as características do *Software* analisador de redes e protocolos Examine da proprietária *Acterna* Inc;

- ✓ Capítulo IV – Especificação dos testes de medições a serem executados, especificação do Cenário de teste e aspectos topológicos - tanto para a topologia física / lógica, bem como a análise da rede da OP inicialmente projetado para fins de testes e funcionalidades dos equipamentos de comutação da Rede;
- ✓ Capítulo V – Resultados parciais das medições laboratoriais, sobre os codecs, cRTP, LFI, análise dos parâmetros da rede como *jitter*, banda ocupada, etc;
- ✓ Capítulo VI – Medições conclusivas correlacionando tráfegos com diferentes Codecs, com e sem compressão RTP, com fragmentação e sem fragmentação, com e sem políticas de QoS; medições com um e dois tráfegos de dados FTP em paralelo com tráfego e voz e testes com dois tráfegos de voz e gráficos comparativos;
- ✓ Capítulo VII – Apresentação das medições conclusivos com tráfegos de diferentes Codecs através da formatação de uma matriz de Resultados, uma seção da análise dos protocolos a nível do domínio Backbone IP/MPLS e finalmente a seção de recomendações de boas práticas;
- ✓ Capítulo VIII – Conclusão da dissertação e a seção dos estudos futuros recomendados;
- ✓ Capítulo IX – Referências Bibliográficas e, Bibliografias Consultadas;
- ✓ Capítulo X - Apêndices – Algumas telas geradas e capturadas durante os testes que ajudam a entender e ilustrar todo o trabalho;
- ✓ Capítulo XI (Anexo) - Neste capítulo serão realizados estudos conceituais sobre: a Tecnologia IP/VPN/MPLS, Fragmentação a nível IP, algoritmos de Fragmentação e remontagem de pacotes, abordando as suas contextualizações no cenário das medições realizadas.

-
- ✓ Capítulo XII (Anexo) - Neste capítulo serão também realizados estudos conceituais sobre os métodos de melhoria e otimização de banda como: Codecs; compressão de cabeçalho RTP (cRTP); Protocolo RTP;
 - ✓ Capítulo XIII (Anexo) – Serão analisadas algumas considerações importantes sobre QoS, sua arquitetura DiffServ; Aspectos de desempenho e otimização de redes de pacotes e os seus algoritmos de escalonamento de filas, estudo e avaliação dos perfis de QoS dos equipamentos Cisco usados;

Dessa forma, seguindo o Título 1.1.1– estrutura da dissertação – fecha-se o Capítulo I capítulo de introdução passando ao Capítulo II que é um dos capítulos que aborda a contextualização teórica sobre esta dissertação e, desta forma, o Capítulo XIII (Anexos) aborda outros conceitos de igual importância a este capítulo, que fazem assim parte desta dissertação.

2 – CAPÍTULO II – REDES FRAME RELAY E RECOMENDAÇÃO SEGUNDO O PADRÃO FRAME RELAY FORUM v12 (FRF.12).

“As coisas não são boas ou ruins; o pensamento é que as faz assim”
– William Shakespeare

2.1 - REDES FRAME RELAY

O padrão para o protocolo Frame Relay tem sido desenvolvido pelo ANSI (*American National Standard Institute*) e ITU-T simultaneamente [30]. As redes FRF, embora tecnicamente obsoletas nos dias de hoje, ainda são praticadas comercialmente por algumas operadoras de telefonia e clientes cujos enlaces são de baixa capacidade, no estudo e testes realizados pelo LOP. Os testes foram realizados sobre uma interface FRF.12 de link – 512kbps. Posto isso, mostra-se necessário introduzir alguns conceitos sobre a tecnologia Frame Relay e as recomendações Frame Relay Fórum v12, conforme abordado mais adiante neste capítulo.

2.1.1 - Frame Relay - Conceito:

Define-se o Frame Relay como sendo um serviço de comunicação de dados baseado na tecnologia de comutação de pacotes (*packet switching*) orientado à conexão, providos por redes de suporte as interfaces de acesso a terminais de usuários. Essa tecnologia assegura serviço com velocidades de acesso de 64kbps a 2Mbps interligando redes dispersas geograficamente que precisam trafegar diferentes tipos de dados.

O FRF, provê a transferência unidirecional e bidirecional de *Service Data Unit* (SDUs) entre duas ou mais interfaces usuários-rede denominados de *User to Network Interface* (UNI) a fim de manter a ordem da entrega das SDUs de uma determinada conexão virtual configurada para um destino específico. Vale destacar, que essa tecnologia – Frame Relay - não utiliza mecanismos de controle de fluxos e de erros, ficando assim, essas funções por conta do usuário. Sendo assim, não há garantia de entrega de todas as SDUs que são transmitidas, podendo descartar parte delas por ocorrência de erros e congestionamento na rede. Entretanto, as operações em Frame Relay dão-se em três fases bem definidas através dos serviços a nível do núcleo da rede [24]:

- ✓ Fase de estabelecimento de conexão;
- ✓ Fase de transferência de dados

✓ Fase de desconexão

A tecnologia Frame Relay proporciona, contudo, uma boa técnica de multiplexagem estatística das comunicações, permitindo que diferentes fluxos compartilhem uma só linha de transmissão.

2.1.2 - Características do Frame Relay

A Figura 1 a seguir, ilustra a arquitetura típica de uma rede Frame Relay.

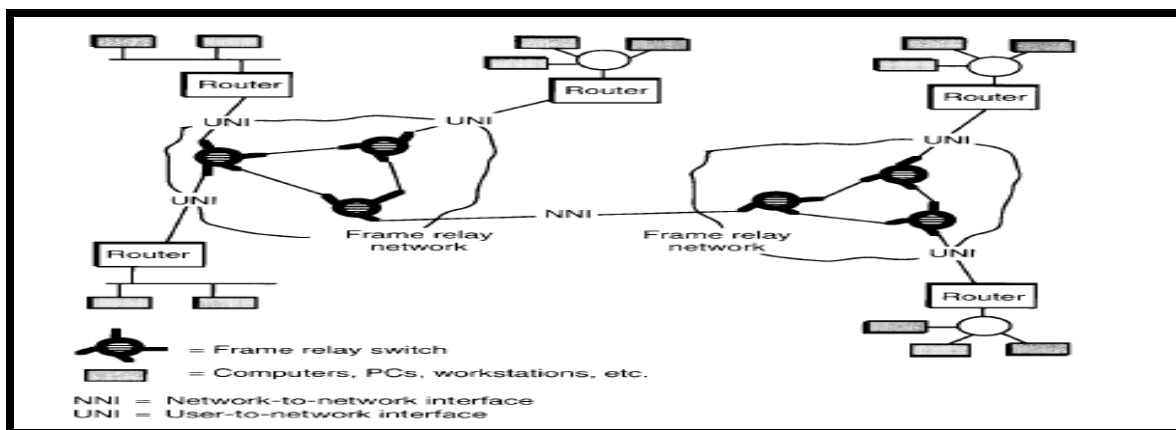


Figura 1 - Frame Relay - Topologia Típica [24]

Em uma rede Frame Relay típica, conforme evidenciada na Figura -1, o dispositivo do usuário é conectado à rede Frame Relay através de um roteador /outro dispositivo de acesso Frame Relay FRAD (*Frame Relay Access Device*) que implementa o protocolo UNI (*User to Network Interface*) [24].

2.1.2.1 - Tipos de Interface

Frame Relay por padrão especifica 2 (dois) tipos de interfaces: UNI e NNI (*Network-Network Interface*) e o analista de redes define a operação interna à rede. As interfaces NNI definem os procedimentos para a interconexão de diferentes redes *Frame-Relay*, tais como:

- ✓ A UNI engloba ainda aspectos como a transferência de informações, a sinalização e a gerência de redes;
- ✓ A transferência de informações diz respeito ao plano de usuário e demais controles como, por exemplo, o controle de fluxo e recuperação de erros;
- ✓ O plano de controle do Frame Relay diz respeito aos processos e funções de controle de chamadas e conexões, envolvendo a sinalização para estabelecimento, supervisão, liberação de chamadas e conexões;

- ✓ O plano de gerenciamento envolve os aspectos e funções concernentes ao gerenciamento das camadas e ao gerenciamento do próprio plano de gerenciamento.

As NNI geram mensagens que são encapsuladas em um quadro de informação não-numerado chamado de HDLC (*High-Level Data Link Control*). Uma vez ocorrido esse procedimento, os bits BECN, FECN e DE não são usados e são assim setados como iguais a zero [24],[25].

2.1.2.2 - Funções Fundamentais:

Para a transmissão de dados entre usuários finais, o protocolo usado é o Q.922 que é uma versão melhorada do LAPD (*Link Access Protocol on the D-channel*). Somente as funções básicas do Q.922, indicadas a seguir, são utilizadas pelo Frame Relay:

- ✓ Delimitação de quadros, alinhamento e transparência (usando *flags* HDLC);
- ✓ Frame de multiplexação e demultiplexação usando o campo *address*;
- ✓ Inspeção do frame para garantir que ele não seja muito longo ou muito curto;
- ✓ Detecção de erros de transmissão usando uma sequência de verificação de quadro (FCS);
- ✓ Funções de controle de congestionamento;
- ✓ A sinalização é feita utilizando LAPD (*Link Access Protocol – on the D-Channel*);
- ✓ Detecção, mas não correção, de erros de transmissão [25] [30].

2.1.3 -Algumas vantagens do Frame Relay:

- ✓ Permite implementar eficientemente a QoS, possibilitando definir prioridades a pacotes de natureza distintas e tráfegos diferentes; Otimização e incremento da eficiência da rede pela utilização de uma única linha de transmissão partilhada por diferentes canais;
- ✓ Possibilidade de integração de tráfego multimídia, permitindo transporte de dados em tempo real, imagens e dados sobre o mesmo enlace;
- ✓ Interoperabilidade com outras tecnologias como ATM;
- ✓ Facilidade em transportar, lidar e gerenciar serviço multimídia, suportando qualquer tipo de aplicação multimídia;

- ✓ Permite constituir rede privada virtual multimídia de suporte a diferentes tipos de tráfego;
- ✓ Proteção do investimento - Frame Relay permite integrar redes legadas, possibilitando que o cliente mantenha a infra-estrutura anterior, sem nenhuma limitação em termos dos benefícios trazidos pelo uso de uma tecnologia mais avançada [84]

2.1.4 - Estrutura de cabeçalho Frame Relay

A estrutura do quadro Frame Relay é baseada no protocolo LAPD. Nessa estrutura, o cabeçalho do quadro é ligeiramente alterado para conter o “*Data Link Connection Identifier*” (DLCI) de 10 bits e *congestion bits*, no lugar do endereço normal e campos de controle. Este novo cabeçalho Frame Relay é de 2 bytes de comprimento e tem o seguinte formato:

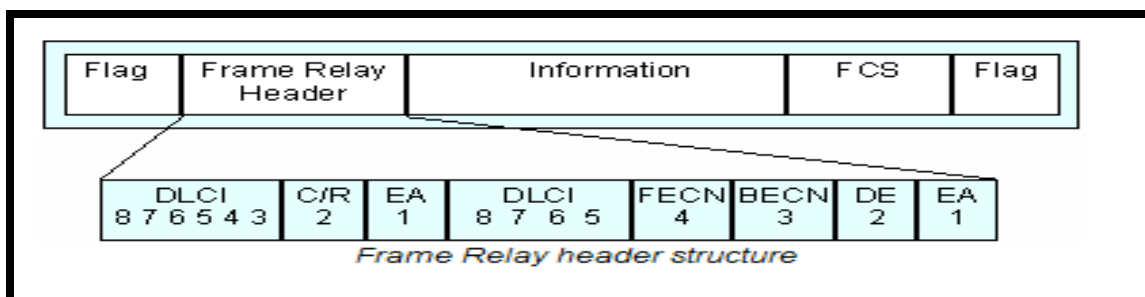


Figura 2 - Cabeçalho de Frame Relay de 2 bytes [30]

Conforme a Figura-2, os campos do cabeçalho DL-Core do Frame Relay têm as seguintes funções [25] [29] [30] [31]:

- ✓ O Bit C/R (*Command/Response*) será utilizado caso esteja operando em modo de controle e gerência no Frame Relay; normalmente este bit não é modificado pela rede;
- ✓ O Bit EA (*Extension Address*) indica o tamanho do campo endereço, sendo zero em todos os octetos, com exceção do último, quando for setado para um. É muito utilizado na sinalização da rede FR (Frame Relay) e ISDN (*Integrated Services Digital Network*);
- ✓ O Bit FECN (*Forward Explicit Congestion Notification*) é setado para valor 1 (um) quando o pacote encontrar congestionamento na rede no mesmo sentido em que a sua transmissão é feita, neste caso o DTE (*Data Terminal Equipment*) do destino é notificado sobre a ocorrência de congestionamento no sentido do quadro;

- ✓ O Bit BECN (*Backward Explicit Congestion Notification*) ao contrário, indica congestionamento no sentido oposto ao do quadro. Esse bit é setado para valor um (1) quando o pacote encontrar congestionamento na rede no sentido contrário ao qual a sua transmissão é feita;
- ✓ O Bit DE (*Discard Eligibility*) se for setado para o valor 1 (um), escolhe o quadro que o contém como sendo o maior candidato e descarta-o em caso de congestionamento ao longo da rede, com relação aos quadros que trafegam com o Bit DE igual a zero (0).

2.1.4.1 - *Data Link Connection Identifier (DLCI)* – Identificador conexão de enlace de dados.

O campo DLCI do frame Relay é usado como identificador do circuito virtual de uma conexão de enlace de dados para identificar o usuário de destino. Esse campo tem um comprimento mínimo de 10 bits embora possa ser ampliado, assinalando-o com os bits EA. Os DLCIs são pré-configurados para o nó de destino.

O roteador encaminha o tráfego com base no valor do DLCI (Para os testes no CRT foi setado o valor a 100), que serve como parâmetro de entrada para consulta à sua tabela de roteamento. Os 10 bits desse campo são semelhantes ao número de circuito virtual de um protocolo de camada de rede, podendo ser expandidos com a opção de endereçamento estendido. A função de conversão de endereços é fundamental para a operação da rede, embora não definida pelo Frame Relay. O DLCI é ainda usado na fase de transferência de dados, permitindo originar 1.024 conexões virtuais em cada um dos enlaces físicos. Dessas 1.024 conexões virtuais, 976 são disponibilizadas para conexões de usuários e 48 para fins de controle e operação da rede. Através dessas conexões virtuais os quadros são enviados, devendo atender aos requisitos de QoS e de tráfego exigido por um determinado ETD solicitante [25], [31].

2.1.5 - Interligação de LANs

A interligação entre as LANs é realizada usando os circuitos virtuais PVC (*Permanent Virtual Circuit*). Com os PVC's - *Frame Relay* é possível criar uma topologia lógica em redes de malha com conectividade similar a da topologia física realizada com circuitos dedicados. Desse modo, é permitida uma partilha eficiente de largura de banda pelos vários circuitos virtuais pertencentes aos fluxos de tráfego entre LANs. Os PVC's permitem que cada LAN requeira um único acesso a um *backbone*

comum, permitindo a redução das manobras de gestão da rede e também a redução do número de interfaces por roteadores interligados [25], [30].

2.1.5.1 - Algumas Mensagens usadas no estabelecimento de PVC (SE, S e FS)

- ✓ *Status Enquiry* (SE): Solicita o status real de um determinado PVC / Enlace físico;
- ✓ *Status* (S): Mensagem¹² que informa o status de um PVC / Enlace físico. É enviada normalmente em resposta a uma mensagem SE;
- ✓ *Full Status* (FS): Informa o status de todos os PVCs em um enlace físico.

2.1.5.2 - Circuitos Virtuais (*Virtual Circuits*)

Um circuito virtual pode ser entendido como sendo um circuito de dados virtuais bidirecionais configurados entre um par de portas quaisquer da rede. Uma vez configurado, este circuito virtual passa a funcionar como um circuito dedicado/delicado.

A tecnologia Frame Relay foi projetada para operar, nativamente, sob forma de circuitos virtuais. Existem, assim, dois tipos de circuitos virtuais em Frame Relay: os SVC's e os PVC's.

2.1.5.2.1 - Circuitos virtuais comutados (*Switched Virtual Circuit* (SVC))

SVC são utilizados em situações que requerem a transferência de dados periódicos entre dispositivos DTE. Por isso, os SVC's são considerados conexões temporárias em enlaces Frame Relay. Por serem conexões não permanentes, uma sessão SVC consiste em quatro procedimentos diferentes [31]:

- ✓ ***Call setup*** - Configurar e estabelecer a chamada de circuito virtual entre dois dispositivos DTE Frame Relay;
- ✓ ***Data transfer*** - Transferência de dados das informações são feitas entre os dispositivos DTE através do circuito virtual;
- ✓ ***Idle*** - A sessão de espera permite preservar a conexão entre dispositivos DTE ainda que esteja ativa, mas não há ainda informações transferidas. Todavia, essa espera é definida por um período de tempo para evitar que a chamada seja encerrada;
- ✓ ***Call termination*** – A sessão de terminação de chamadas permite encerrar o circuito virtual entre dispositivos do DTE frame Relay. Após o encerramento do

¹² **Mensagem:** Unidade de informação que a Camada de Aplicação passa para a Camada de Transport

circuito virtual, os dispositivos DTE devem estabelecer um novo SVC, caso existirem mais dados a serem trocados. Feito isso, espera-se que os SVCs sejam estabelecidos, mantidos e encerrados com os mesmos protocolos de sinalização utilizados em ISDN.

2.1.5.2.2 - Circuitos virtuais Permanentes (*Permanent Virtual Circuit (PVC)*)

O PVC foi o primeiro tipo de circuito virtual padronizado para o Frame Relay a ser implementado. Ele é configurado pelo operador na rede através do sistema de Gerência de Rede, como sendo uma conexão permanente entre 2 (dois) DTE's. O seu encaminhamento através dos equipamentos da rede pode ser alterado ao longo do tempo devido às falhas ou reconfigurações de rotas. Porém, as portas de cada extremidade são mantidas fixas e de acordo com a configuração inicial.

A configuração dos PVC's requer um planejamento criterioso para levar em consideração o padrão de tráfego da rede e o uso da banda disponível. A sua utilização é destinada às aplicações permanentes e de longo prazo e são uma alternativa aos circuitos dedicados dos sistemas TDM com boa relação custo / benefício.

2.1.6 - Controle de Tráfego em Frame Relay

O mecanismo de controle de tráfego em Frame Relay tem como objetivo evitar o congestionamento na rede de suporte. Para tal, as redes Frame Relay dispõem de dois mecanismos básicos: Policiamento do tráfego e Notificação de congestionamento. O mecanismo de policiamento de tráfego dispõe dos seguintes parâmetros de tráfego:

- ✓ *Committed Information Rate (CIR)*;
- ✓ *Committed burst size (Bc)*;
- ✓ *Excess burst size (Be)*;
- ✓ *Access Rate (Ar)*

2.1.6.1 – Descrição dos parâmetros de Tráfego Frame Relay

- ✓ **AR:** É a capacidade do canal físico em acessar aos serviços. O valor da capacidade disponibilizada pelo utilizador é limitado pela capacidade do canal de acesso.
- ✓ **CIR:** Diz respeito ao valor mínimo garantido na interface de acesso que a rede deve garantir em condições normais aos usuários. A rede transporta o tráfego que ultrapassa CIR desde que não haja congestionamento. Entretanto, o valor

específico do CIR deve ser negociado no ato do contrato de prestação do serviço. A rede monitora o tráfego do usuário e se o tráfego ultrapassar o valor CIR, os Bits DE são setados iguais a 1 (um), tornando os quadros elegíveis para descarte em caso de congestionamento.

- ✓ **BC:** É o valor máximo da quantidade de informação que a rede pode aceitar para ser transferido em condições normais durante um intervalo de tempo que pode ser definido pela relação $BC = CIR * T$. O BC pode permitir transmitir uma rajada (*burst*) máxima BC com valor instantâneo de AR, se o valor médio não exceder o CIR.
- ✓ **BE:** Para além do BC, o BE é a máxima quantidade de informação que a rede pode transmitir condicionalmente durante um intervalo de tempo T. Assim o Be pode ser dado pela relação $BE = EIR * T$, onde: EIR - *Excess Information Rate*.

A rede mede constantemente a quantidade de bits em cada circuito virtual, a fim de policiar se a quantidade de bits medida está sendo menor que o BC ou não. Se for menor, o tráfego do circuito virtual entra normalmente na rede, com o bit DE igual a zero (0) permitindo ao tráfego uma menor probabilidade de descarte. Se, se verificar o contrário, isto é, a quantidade de bits for maior que BC e menor que a soma do Bc e Be, dir-se-á que o limite do CIR não foi respeitado pelo usuário. Entretanto, ficará claro que foi mantido o tráfego dentro dos limites aceitáveis. O tráfego Bc entra na Rede com o bit DE igual a zero. Por seu turno, o Be entra na Rede com o bit DE igual a 1 (um), a fim de identificar os quadros que, em uma situação de congestionamento, seriam descartados em primeira mão. Em situação adversa, em que os limites são ultrapassados como, por exemplo, a soma Bc e Be, com o tráfego Bc tratado normalmente, o tráfego Be é aceite para entrar na rede mas, com maior probabilidade de ser descartado. O tráfego Bc somado do Be é descartado independentemente da situação de congestionamento da Rede no momento, pois o algoritmo de balde furado (*Leaky-Bucket*) é utilizado no policiamento do tráfego na entrada do circuito virtual. [9],[16],[31].

2.1.7 - Controle de Congestionamento

De entre os principais objetivos do controle de congestionamento em redes Frame Relay, destacam-se os seguintes:

- ✓ Notificar a ocorrência de congestionamento com o objetivo de fazer com que o DTE reduza a taxa de transmissão do tráfego, minimizando assim o descarte de quadros;
- ✓ Manter, com alta probabilidade e mínima variação, o acordo de QoS firmado;
- ✓ Evitar que ocorram sobrecargas sobre os usuários finais;
- ✓ Limitar a propagação de congestionamento para outras redes e elementos da rede;
- ✓ Operar de forma eficaz, independentemente do fluxo de tráfego em qualquer direção entre os usuários finais;
- ✓ Procedimentos para evitar congestionamento são adotados no início de congestionamento para minimizar o efeito na rede. Isso exige sinalização explícita pela rede antes de serem descartados grandes volumes de informações [25].

2.1.8 - Moldagem e Policiamento de Tráfego

Para controle e moldagem de tráfego em redes Frame Relay, utiliza-se o FRTS (*Frame Relay Traffic Shaping*), que permite manipular parâmetros úteis de cabeçalho Frame Relay, como o CIR (*Committed Information Rate*), o EIR (*Excess Information Rate*), o FECN (*Forward Explicit Congestion Notification*), o BECN (*Backward Explicit Congestion Notification*) e o DE (*Discard Eligible*), conforme anteriormente descrito.

Com FRTS pode-se, por exemplo, limitar no CIR ou o EIR à taxa de pico do tráfego de saída em cada VC (*Virtual Circuit*), procedimento denominado *Rate Enforcement*. Pode-se obter uma maior granularidade no controle de tráfego, aplicando técnicas de enfileiramento como PQ (*Priority Queueing*) ou CQ (*Custom Queueing*) [8] em cada VC ou no nível de sub-interface. Combinando CQ e enfileiramento por VC com *Rate Enforcement*, pode-se habilitar o VC a acomodar vários tipos de tráfego como IP, SNA e IPX, cada um com sua própria banda garantida [9].

2.1.9 - Moldagem Genérica

Generic Traffic Shaping (GTS) - oferece mecanismos para controle de tráfego através da utilização de filtros do tipo *token bucket*¹³, limitando assim o tráfego de saída de uma interface a uma determinada taxa. A Figura - 3 a seguir mostra o tráfego a ser

¹³ **Token Bucket** é uma maneira formal para definir a taxa de transferência

classificado seguindo a um *buffer* limitador, sendo liberado sob regras pré-definidas de acordo uma política de controle de tráfego, que pode ser configurada pelo administrador ou derivada da interface [12].

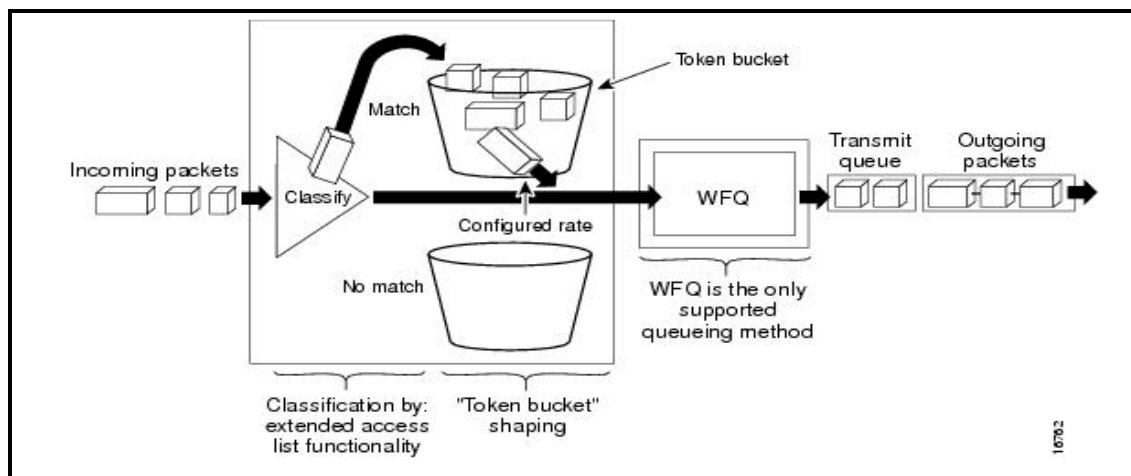


Figura 3: Generic Traffic Shaping [12].

A moldagem ou conformidade de tráfego (GTS) pode ser útil em vários casos. Por exemplo, para limitar o tráfego de rajada de forma a não prejudicar o tráfego prioritário reduzindo, assim, a latência, ou, em situações de congestionamento, para limitar um determinado tipo de tráfego não sensível a retardo, como transferência de arquivos eliminando possíveis gargalos. A moldagem GTS aplica-se apenas em interfaces de saída, com o uso de listas de acesso para classificar e selecionar o tráfego, podendo funcionar com qualquer tecnologia de enlace (nível-2) como Frame Relay, ATM (*Asynchronous Transfer Mode*), Ethernet entre outras.

O *Token bucket* possui três parâmetros básicos:

- ✓ *Burst size* (tamanho de rajada em bits), também chamado de *committed burst* (Bc) que especifica o quanto pode ser enviado num determinado intervalo de tempo;
- ✓ *Mean rate*- (taxa média em bps), ou CIR (*Committed Information Rate*), que especifica o quanto em termos de dados, em média, pode ser enviado por unidade de tempo;
- ✓ Tc – (Intervalo de tempo em sec), especifica o tempo por rajada [12].

2.1.9.1 – Policiamento

O CAR (*Committed Access Rate*) é uma metodologia usada para controle e policiamento de tráfego IP que realiza, basicamente, duas funções para a qualidade de serviço:

- ✓ Gerenciamento de banda com limitação de taxa de acesso (*policing*) - permite controlar a taxa máxima de transmissão ou recepção de dados de uma determinada interface. O tráfego conforme é transmitido ou recebido, enquanto que os pacotes que excedam os limites pré-definidos, são descartados, ou reclassificados com outra prioridade;
- ✓ Classificação de pacotes através de precedência IP ou de grupos de QoS (um rótulo interno do roteador utilizado para definição de classes) permite particionar a rede em múltiplas classes de serviços ou níveis de priorização [13].

O CAR paralelamente ao mecanismo de *token bucket*, examina o tráfego recebido na interface ou parte do tráfego selecionado pelos critérios das listas de acesso, compara a taxa de tráfego com a do *token bucket* (Figura-4 a seguir) e, de acordo com o resultado, toma as ações, podendo transmitir o pacote, descartá-lo ou reclassificá-lo com outro nível de prioridade.

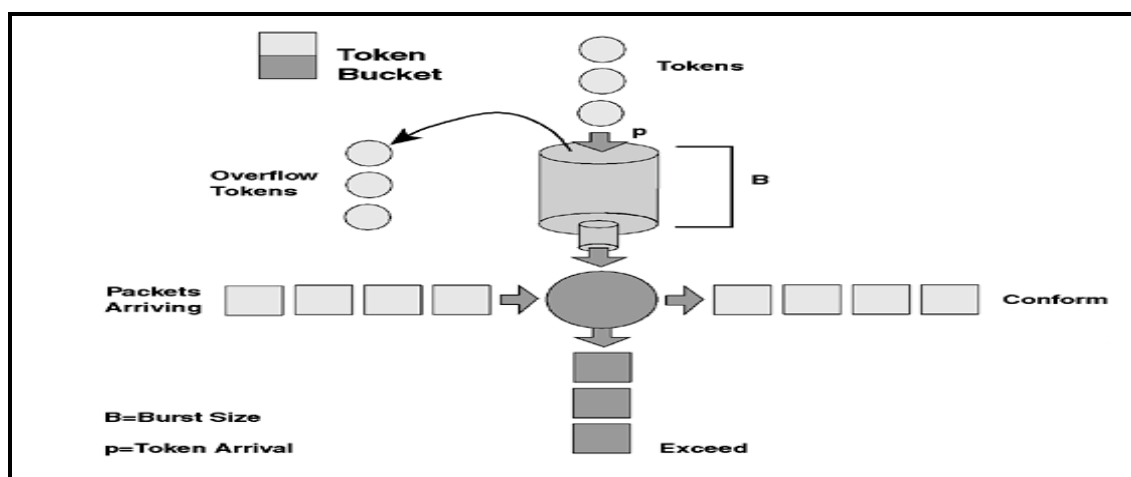


Figura 4 - Committed Access Rate com token bucket [13].

Os *tokens*¹⁴ são inseridos no balde na mesma taxa CIR. A profundidade do balde é o tamanho da rajada (*burst size*). Se houver *tokens* suficientes quando o tráfego chega

14

Token: Um segmento de texto ou símbolo que pode ser manipulado através de um processo de análise de uma entrada sequencial que fornece um significado ao texto; Um token pode também ser entendido como sendo um conjunto de caracteres.

ao balde, diz-se que o tráfego está em conformidade e a quantidade correspondente de *tokens* é removida. Se não houver *tokens* suficientes, então diz-se que o tráfego é excessivo. Os critérios de seleção de tráfego podem ser baseados em todo tráfego IP, em precedência IP, em listas de acesso (padrão ou estendida), em endereço MAC (*Media Access Control*) ou, ainda, em grupos de QoS. O endereço MAC e a precedência IP podem ser definidos através de listas de acesso *rate-limit*.

Com o CAR, pode-se limitar o tráfego por aplicação (Web, FTP, entre outros), por interface (por exemplo, uma conexão serial a 2 Mbps, mas com acesso limitado em 512 Kbps), por endereço MAC (por exemplo, controle de tráfego em PTT - Pontos de Troca de Tráfego), ou pode-se classificar ou reclassificar todo o tráfego de entrada num *backbone* a partir dos roteadores de borda, para tratamento diferenciado em termos de qualidade de serviços [7], [4],[9].

Todas essas técnicas do Frame Relay, anteriormente descritas, são aplicáveis a recomendação FRF.12. Essa recomendação acrescenta tratamentos específicos a fluxos de frames de voz entre os pacotes, através da intercalação desses entre os fragmentos de dados FTP. A subseção seguinte discute as metodologias FRF.12.

2.2 - **FRAME RELAY FORUM v12 (FRF.12)**

A tecnologia Frame Relay, embora pouco usada nos dias de hoje, continua a ser uma poderosa ferramenta usada em redes de telecomunicações para prover alguns serviços baseados em circuitos virtuais específicos a alguns clientes específicos. Nessa perspectiva, a Frame Relay desenvolveu metodologias próprias a ela agregadas como o caso da recomendação FRF.12, cujo uso se destina ao tratamento de tráfegos específicos em uma rede de acesso de banda compartilhada. Nasce, assim, o Padrão “*Frame Relay Fragmentation Implementation Agreement*”- FRF.12, também conhecido como FRF.11, cuja finalidade é prover funcionalidades para “*Link Fragmentation and Interleaving*” – *LFI* em enlaces orientados a conexão ponto-a-ponto de baixa capacidade, permitindo a fragmentação fim-a-fim e “*interleaving*” (*intercalação*) de *frames* num mesmo VC (*Virtual Circuit*). A sua utilização é assim não recomendada nos VCs que trafegam voz, mas sim nos VCs de dados que compartilham a mesma conexão física de voz onde a banda máxima costuma ser de até 2Mbps. Esses VC's podem ser SCV ou PVC, conforme p.ex. o frame relay prevê em suas implementações.

2.2.1 - Implementação de LFI em acesso Frame Relay (FR).

Nas tecnologias de rede de acesso FR, duas formas de implementação de LFI podem ser consideradas: a MPPP (*Multilink PPP*) e o FRF.12 do Frame Relay Fórum. Nos testes realizados não foram implementados as metodologias MPPP, mas sim as metodologias FRF.12, dando, mais ênfase ao FRF.12 e às suas técnicas de QoS.

2.2.1.1 – Outras considerações sobre a LFI de pacotes no nível do enlace Frame Relay.

Na camada IP ocorre a fragmentação de pacotes sempre que necessário, embora sem intercalação de pacotes de voz. Os pacotes de voz sobre IP não podem ser fragmentados mas sim intercalados habitualmente no nível de enlace entre os pacotes de dados, por exemplo. Na camada IP são fragmentados pacotes de dados, usando protocolos como Ethernet cuja MTU é de 1500 bytes, tamanho esse superior a MTU máxima de 640bytes [20] em um link de enlace de 512Kbps usado no laboratório da OP.

Percebe-se, então, que uma MTU de 1500bytes de uma interface LAN Fast Ethernet que opera na ordem de transmissões de 10/100 Mbps carregaria, provavelmente, pacotes maiores que a interface de enlace. Esses pacotes grandes prejudicariam um pacote pequeno de voz quanto ao tempo de serialização¹⁵, aumentando o *jitter* para uma aplicação sensível ao atraso. Para isso a técnica empregada foi de intercalação dos pacotes de voz entre os fragmentos de dados. Não seria portanto, proveitoso se a referida técnica fosse aplicada sobre uma MTU de 1500bytes, isto é, se a fragmentação interleaving ocorresse sobre o nível-3. Para que isso venha a ser aceitável e ser, em parte, realmente útil, teríamos que decrementar a MTU do protocolo Ethernet de 1500 bytes a um valor inferior a pelo menos ao MTU do enlace. Além disso, precisa-se necessariamente modificar e adaptar a configuração das interfaces dos roteadores para que se tenha *Interleaving* em nível IP. Perante essas considerações, ter-se-ja que lidar com, pelo menos, algumas das vantagens e desvantagens seguintes:

Como vantagens tem-se, entre outros:

- Reduzir o processamento no nível-2;
- Alocar o nível de enlace a outras tarefas;
- Garantir e manter a QoS, etc

15

Serialização: ‘E o atraso de bloqueio que um *frame* de voz sofre para ser inserido entre os datagramas FTP. ‘E o intervalo entre o envio e a inserção (recepção) do frame de voz.

Como desvantagens temos:

- Aumentar o processamento no nível-3 devido a quantidades de pacotes a serem tratados e transportados;
- Aumentar drasticamente a quantidade de cabeçalho no nível 3
- Carga útil e “lixo” – cabeçalho em proporções simétricas;
- Cai o desempenho da interface Fast-Ethernet, uma vez que carrega datagramas de tamanho menor que o recomendado.
- Sub-utilização da banda passante da rede, etc...

É muito importante enfatizar que o procedimento de fragmentação com intercalação (*Interleaving*) de pacotes, como por exemplo voz, não existe na prática no nível do IP, ou seja, camada de rede. O que ocorre na prática é a sua utilização no nível 2 (dois).

2.2.2 - Multilink PPP

A ativação LFI requer a configuração do MPPP com *interleaving* e encapsulamento PPP (*Point-to-Point Protocol*), permitindo que grandes pacotes sejam fragmentados para satisfazer os requisitos de retardo do tráfego de voz. Os pacotes menores, que não são encapsulados no *multilink*, são transmitidos entre os fragmentos dos pacotes maiores. Ao ativar a funcionalidade para *interleaving*, uma fila especial é alocada para o tráfego sensível a retardo, provendo certa priorização. Nos roteadores Cisco, o MPPP é ativado através de um *template* de interface virtual [1]. Em geral, o MPPP é utilizado em conjunto com WFQ e precedência IP ou RSVP (*Resource Reservation Protocol*), para assegurar qualidade de serviço na transmissão do pacote. O seu uso, entretanto, não é recomendado em conexões maiores que 2 Mbps [15].

2.2.3 – LFI Especificação - Frame Relay Fórum v12 (FRF.12)

Em voz sobre IP, os pacotes não devem ser fragmentados, mas podem ser intercalados entre os fragmentos. É também importante que o tráfego de voz sobre IP não exceda a CIR (*Committed Information Rate*) do PVC Frame Relay, o que pode degradar a qualidade do sinal. Para isso, pode-se utilizar o FRTS (*Frame Relay Traffic Shaping*). Quando a fragmentação é utilizada com tráfego FRF.11, que é a implementação do Frame Relay Fórum para VoFR (*Voice over Frame Relay*) - Voz sobre Frame Relay, os dados são transmitidos no formato FRF.11. Nesse caso, independentemente do tamanho, todos os pacotes de dados irão conter cabeçalho de fragmentação. Esse tipo de fragmentação não é recomendado para uso com voz sobre

IP. Daí que se aplique a FRF. 12, que dispõem de melhores tratamento de VoFR [1],[2],[4].

A fragmentação reduz filas, tanto atraso e jitter em redes Frame Relay, dividindo grandes pacotes de dados em pacotes menores e depois remontar os dados para os quadros originais no destino. Essa capacidade é particularmente relevante para os usuários que desejam combinar voz e outras aplicações sensíveis ao tempo, tais como aplicações de missão crítica SNA, com aplicações não-sensíveis ao tempo ou outros dados em um único circuito virtual permanente (PVC).

O benefício principal da fragmentação é a capacidade de utilizar *User Network Interface* (UNI) comum para as linhas de rede acesso para interface de rede (NNI) linhas e / ou PVC para as comunicações que combinam grandes quadros de dados e protocolos em tempo real [14],[9]. O FRF.12 suporta três aplicações de fragmentação:

- ✓ Localmente através de uma interface Frame Relay UNI entre os pares DTE (*Data Terminal Equipment*) e DCE(*Data Communications Equipment*);
- ✓ Localmente através de uma interface Frame Relay NNI entre os pares;
- ✓ *End-to-End Frame Relay (FR)* entre dois DTEs interligados por uma ou mais redes FR.

Quando usada de ponta a ponta, o processo de fragmentação é transparente para redes Frame Relay entre os DTEs de transmissão e recepção [2], [21], [30].

2.2.4 – Técnicas de Fragmentação e Intercalação á Nível de Enlace FRF.12

A fragmentação e intercalação são realizadas no nível dois (L2) quando se tem, normalmente, processamentos de pacotes e frames de tamanhos e tipo diferentes disputando o meio de transmissão. Normalmente a intercalação ocorre quando há presença de frame de tempo real com voz entre os pacotes de dados de tipo FTP.

Os frames de voz são intercalados aos demais pacotes de dados que são naturalmente de capacidades maiores, ocupando mais banda e fazendo com que outras aplicações permaneçam mais tempo na fila, o que não costuma ser uma prática

recomendada, dado o baixo limite de sensibilidade de aplicações do tipo voz se elas forem submetidas a altas variações de atraso.

A prática de intercalação de pacotes permite que pacotes de voz sejam incluídos entre os fragmentos de dados, de forma que uma aplicação de voz não seja prejudicada com longo tempo na fila (esperando, por exemplo, que termine a transmissão de aplicação do tipo FTP se este estiver na frente) e grandes atrasos de serialização para ser transmitida.

Essa técnica faz com que o *delay* (retardo), a variação do retardo (*jitter*) sejam bastante reduzidos, dando a aplicação uma qualidade melhor. Conforme dito anteriormente, essa técnica corresponde ao tipo de operação bastante útil em termos de provisão de QoS, uma vez que se consegue, ainda que com uma banda estreita, prover por exemplo serviços do tipo multimídia e de tempo real com boas qualidades.

O atraso fim-a-fim máximo para pacotes de tempo real tipo aplicações de voz, especialmente, vai até um Máximo de 150ms a 200ms. Não deve haver jitter acima dos 20ms em média, pois degradaria a qualidade do sinal.

Por vezes, mesmo a implementação de mecanismos QoS (*Quality of Service*), WFQ (*Weighted Fair Queuing*) ou PQ (*Priority Queuing*) não tendo sido suficiente para oferecer à aplicação um tratamento adequado com relação ao atraso, imposto às aplicações de tempo real devido à presença na rede de pacotes de diversos tamanhos como, por exemplo, o FTP que pode utilizar pacotes no tamanho da MTU do enlace 1500 bytes.

A transmissão de um pacote de 1500 bytes num enlace de 56Kbps levaria, aproximadamente, 214ms. Isso poderia influenciar de maneira negativa as aplicações de tempo real, conforme ilustra a Figura 5 - a seguir. Esses pacotes poderiam demorar 214ms¹⁶ num enlace para chegar ao receptor e isso excede atraso máximo fim-a-fim de 150ms, segundo a recomendação da ITU-T.

16

Para chegar a este valor em *ms* é usada a seguinte fórmula:

Atraso de serialização (ms) = Tamanho do Frame (bits) / Largura da banda (bps)

*Exemplo: $[(1500 * 8 * 10^3) \text{bits} / (56 * 10^3) \text{bps}] = (214 \text{ms})$*

Os mecanismos de filas não poderiam fazer nada para evitar isto [14],[20].

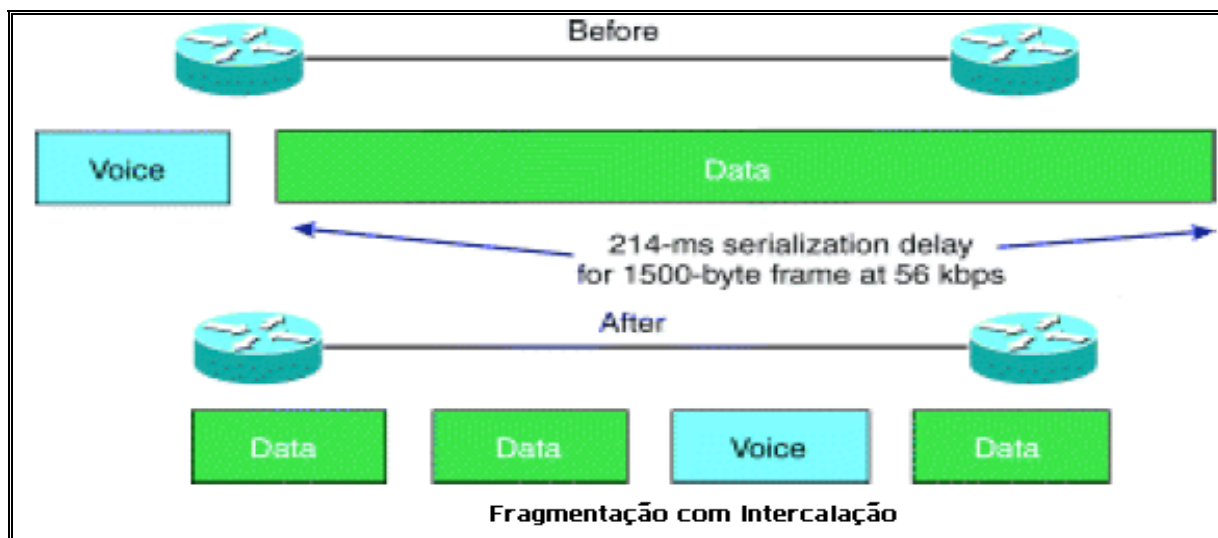


Figura 5 - Fragmentação e intercalação - readaptado [20].

A solução seria fragmentar os pacotes grandes de tal forma que não excedam o atraso fim-a-fim de 150ms e intercalar os pacotes das aplicações de tempo real, com voz e os pacotes de dados que foram fragmentados segundo representa a Figura 5, ou seja, enquanto que 1500 bytes é o tamanho comum dos pacotes de dados, um pacote típico de VoIP (*Voice Over Internet Protocol*) provido pelo codec G.729 pode ter a volta de 66 bytes, (sendo 20 bytes de *payload* de voz, 6 bytes de cabeçalho nível 2, 20 bytes de cabeçalho RTP e UDP (*User Datagram Protocol*) e 20 bytes de cabeçalho IP).

Imagine-se, agora, um link de canal de comunicação de 56kbps alugada onde coexiste o tráfego de dados e voz. Se o pacote de voz acabar de ser serializado quando um pacote de dados começar a ser transmitido sobre o link, então, haverá um problema.

O retardo sensível do pacote de voz terá que esperar 214ms antes de ser transmitido (isso tomará 214ms para serializar pacotes de 1500 bytes sobre um link de 56kbps) [20]. Conforme se pode verificar, grandes pacotes de dados podem chegar com *delay* desfavorável a pequenos pacotes de voz, reduzindo a qualidade da fala.

A Figura 6 - que se segue representa um exemplo típico sobre a ilustração teórica da LFI, onde vários tráfegos diferentes são direcionados a uma interface FRF.12, sendo os mesmos tráfegos classificados por fluxos e colocados em uma fila apropriada recebendo o tratamento de um algoritmo de escalonamento, por exemplo, PQ e WFQ e posteriormente

serão colocados em um *buffer* de fila de transmissão de forma intercalada e encaminhados às respectivas interfaces de saída [20], [70].

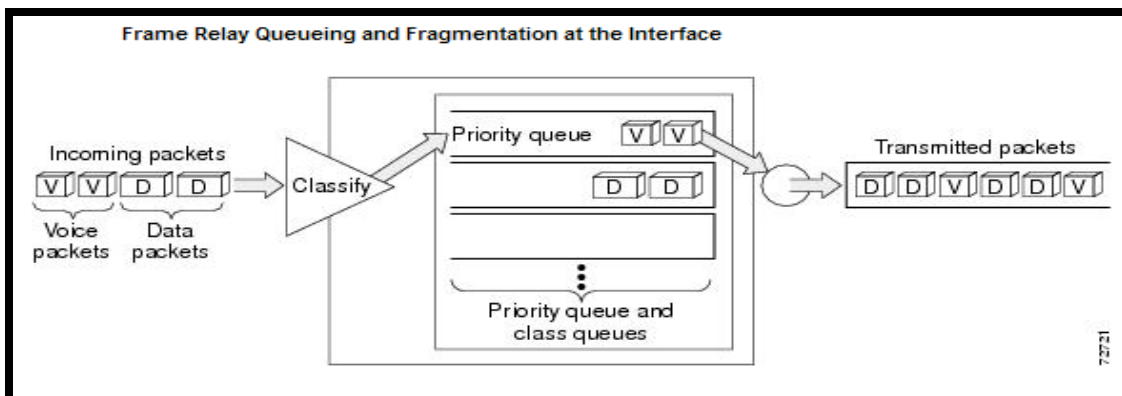


Figura 6 - Processo de enfileiramento dos pacotes na interface FRF.12 e LFI [1]

Fragmentando estes pacotes de dados grandes em pedaços pequenos e intercalando pacotes de voz entre os fragmentos reduz o *delay* e o *jitter* [1], [15]. O LFI reduz o atraso em enlaces de baixa velocidade, fragmentando os pacotes grandes e intercalando os pacotes fragmentados resultantes com os pacotes de tempo real.

O LFI é realizado utilizando duas técnicas: a primeira técnica consiste na implementação MLPP (*Multilink Point-to-Point Protocol*) que suporta a fragmentação e o seqüenciamento do pacote: a segunda técnica utilizada é a Fragmentação Frame Relay (FRF.11 e a FRF.12).

A técnica FRF.12 é a tecnologia em que se baseiam os testes práticos no LOP.

O atraso máximo fim-a-fim para uma aplicação de voz não deve ultrapassar 150ms a 200ms ou o limite 250ms, a fim de impedir uma comunicação de voz / áudio sem sincronismo entre os participantes. A rede deverá, também, garantir um *jitter* pequeno, a fim de não aumentar ainda mais o retardo, ao atrasar o ponto de reprodução dos pacotes para eliminar o *jitter* através de um *buffer* de recepção.

Por outras palavras, os pacotes devem chegar em intervalos de tempo constantes de no máximo 20ms. Não deve haver variação de atraso que comprometa esses valores.

Para a transmissão de um pacote de tempo real, deve ser calculado o tempo que o receptor terá de esperar para receber o pacote. Deve-se considerar o pior cenário, ou seja, pacote fragmentado de dados que foi transmitido um pouco antes que o pacote de voz [15].

A Figura 7 - a seguir esquematiza um cenário típico, considerando, por exemplo, um link muito baixo – 64kbps.

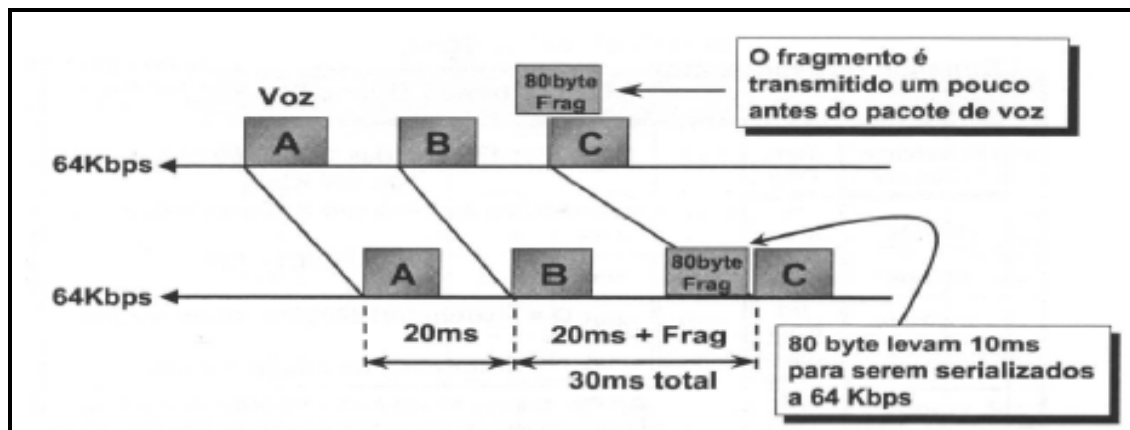


Figura 7 - Atraso de serialização dos pacotes em um link de 64kbps (Readaptado)[20].

Da Figura 7 - pode-se fazer as seguintes interpretações: os pacotes de voz são transmitidos a cada 20ms; os pacotes A e B foram transmitidos; o fragmento de dados de 80 bytes foi transmitido um pouco antes do pacote de voz C. Portanto, o pacote C terá de esperar 10ms para transmitir o pacote de dados de 80 bytes. Isso implica que o bloqueio total do pacote de voz seja de 30ms.

Segundo a correlação matemática evidenciada na Tabela 1 a seguir, estes 30ms podem degradar a qualidade do sinal de voz, uma vez que os 80bytes levam por *default*¹⁷ 10ms para serem serializados a 64kbps, conforme a **Error! Reference source not found.** [11],[3].

Coder		Payload Size (Bytes)	Packetization Delay (ms)	Payload Size (Bytes)	Packetization Delay (ms)
PCM, G.711	64 Kbps	160	20	240	30
ADPCM, G.726	32 Kbps	80	20	120	30
CS-ACELP, G.729	8,0 Kbps	20	20	30	30
MP-MLQ, G.723.1	6,3 Kbps	24	24	60	48
MP-ACELP, G.723.1	5,3 Kbps	20	30	60	60

Tabela 1 - Delay de pacotização por tamanho de *payload* [3]

A Tabela 2 - a seguir demonstra o procedimento de cálculo do tamanho de fragmento, levando em conta velocidades de enlaces bastante diferentes, assumindo atraso considerável de bloqueio em 10ms [14]. O tamanho da MTU no enlace Frame Relay,

¹⁷

Default - Valor usado por não ter outra opção

contrariamente à MTU *Ethernet* de 1500bytes, é dimensionado de acordo com a Tabela 3 - a seguir, sendo assim em um enlace de 512kbps, o tamanho Máximo da MTU a ser reservado é de 640bytes.

Lowest Link Speed in Path	Recommended Fragmentation Size (for 10 ms Serialization)
56 Kbps	70 bytes
64 Kbps	80 bytes
128 Kbps	160 bytes
256 Kbps	320 bytes
512 Kbps	640 bytes
768 Kbps	1000 bytes
1536 Kbps	1600 bytes

Tabela 2 - Cálculo do tamanho do fragmento [20]

Na Tabela 2, assumindo um bloqueio de 10ms de atraso de serialização (atraso de bloqueio), o tamanho da MTU do enlace varia de acordo com a capacidade da banda disponível na rede. Dessa forma, para melhor se entender o dimensionamento do tamanho do fragmento é utilizada a seguinte fórmula (Tabela 3) que também especifica o tamanho máximo da MTU do Enlace. No caso da OP a MTU de enlace é de 640bytes, dado que o link de acesso ao backbone é de 512kbps.

$$\begin{aligned} \diamond \text{ Tamanho Máx.} &= 10\text{ms} / (\text{tempo para transmitir 1 byte na banda do enlace}) \\ \diamond \text{ MTU Máximo} &= 10\text{ms} / (8\text{bytes} * 512000\text{bytes}) = 640\text{bytes}, \end{aligned}$$

Tabela 3- Demonstração do cálculo do Tamanho máximo de MTU de enlace

De acordo com a Tabela 3, pode-se afirmar que nada impede que o administrador da rede limite este tamanho para um valor inferior, reduzindo o tamanho da MTU.

Na matriz a seguir - Tabela 3 - estão os resultados desta fórmula, que são uma correlação entre o tamanho do frame e a velocidade do enlace. Portanto se houver quatro chamadas utilizando, por exemplo, o codec de áudio G.729, serão gerados pacotes com tamanho, em média, de 60 a 66 bytes (480 bits).

Para aplicações de voz, a serialização do *delay* recomendado é de 10ms e não deverá exceder a 20ms. Portanto, o pior caso para um atraso seria de 25ms.

		TAMANHO DE FRAME						
E L A C E		1 Byte	64 Bytes	128 Bytes	256 Bytes	512 Bytes	1024 Bytes	1500 Bytes
	56 kbps	143 us	9 ms	18 ms	36 ms	72 ms	144 ms	214 ms
	64 kbps	125 us	8 ms	16 ms	32 ms	64 ms	126 ms	187 ms
	128 kbps	62.5 us	4 ms	8 ms	16 ms	32 ms	64 ms	93 ms
	256 kbps	31 us	2 ms	4 ms	8 ms	16 ms	32 ms	46 ms
	512 kbps	15.5 us	1 ms	2 ms	4 ms	8 ms	16 ms	32 ms
	768 kbps	10 us	640 us	1.28 ms	2.56 ms	5.12 ms	10.24 ms	15 ms
	1536 kbps	5 us	320 us	640 us	1.28 ms	2.56 ms	5.12 ms	7.5 ms

Tabela 4 – Tempo de retardo de bloqueio dos pacotes por banda disponível (readaptada) [15]

A matriz da Tabela 4 - mostra o tempo de retardo de serialização para vários tamanhos de frames em links de baixa velocidade com *retardo de serialização* = *frame size (bits) / link bandwidth (bps)* [15],[11],[14].

Para atingir o objetivo pretendido, não adianta apenas implementar o FRF.12. É necessário, também, adotar outras técnicas que dão suporte a provisão de serviços VoIP de qualidade como a avaliação e escolha de codecs, compressão RTP, implementar boas práticas de QoS, entre outras técnicas. Dado isso, o capítulo seguinte trata de algumas questões específicas dessas facilidades técnicas – Codecs e cRTP e, conseqüentemente, no capítulo seguinte são analisadas algumas características de QoS propriamente dita.

3 - CAPÍTULO III – CARACTERÍSTICAS DOS SOFTWARES DE MEDIÇÕES

*“Triste não é mudar de idéia.
Triste é não ter idéia para mudar.” Francis Bacon*

Dois importantes softwares foram de fato indispensáveis e utilizados para a realização dos testes de medições. São eles: O MGEN que é um *software free* e o Examine v3.2 - Software proprietário disponível em equipamento próprio a Acterna Examine do fabricante Acterna Inc.

3.1 - MGEN - (*MultiGenerator*) *Free Software*

O software MGEN é um software de plataforma *free* usado para gerar tráfegos unicast bem como multicast em uma rede de pacotes. É também usado para coletar tráfegos anteriormente gerados para fins de estatísticas e análises. Sendo assim, é apresentada uma descrição síntese do gerador MGEN.

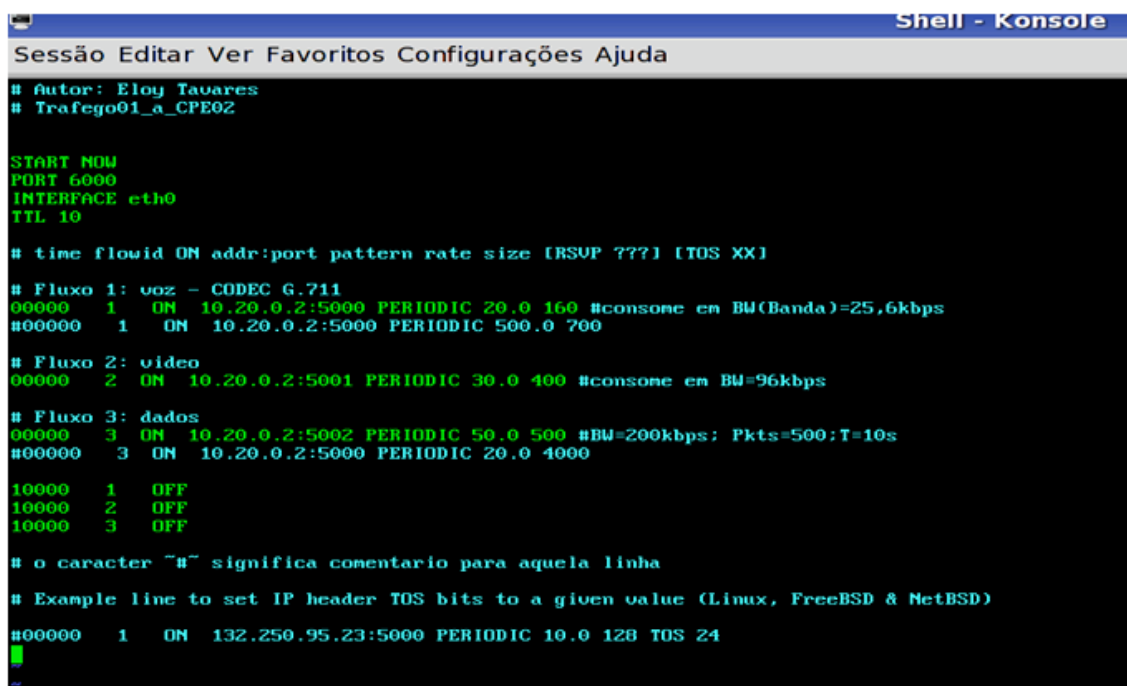
3.1.1 - Características Importantes do MGEN

O MGEN permite gerar e medir tráfego UDP tanto unicast quanto multicast; possui suporte para o protocolo RSVP e permite a criação de scripts utilizando o campo TOS do cabeçalho IP. É multi-plataforma, sendo atualmente suportado pelos seguintes Sistemas Operacionais: *SunOS 4.1.x e Solaris 2.x, Linux, Solaris*i386, NetBSD e FreeBSD*. Existe ainda uma versão para a plataforma Win32.

O MGEN é constituído basicamente por duas aplicações principais, *3mgen* e *drec*, e pelos utilitários *mcalc*, *rcalc*, *allcalc*, *EZ* e *Txdelay*. O MGEN (*Multigenerator*) gera padrões de tráfego e o *drec* (*Dynamic receiver*) recebe e armazena o tráfego gerado. O *mcalc* (*Multicalculator*) mostra estatísticas do tráfego recebido. O *rcalc* é um visualizador gráfico dos níveis de tráfego por fluxo. O *allcalc* gera fluxo estatístico incluindo a taxa média de pacote, a taxa média de bit e a taxa média de atraso. O *scrip EZ*, ao ser executado, gera um arquivo em formato *gif* para ser utilizado pela ferramenta *gnuplot1*. O *Txdelay* produz um arquivo texto que registra o atraso de transmissão em função do tempo [18].

A geração do tráfego é realizada através de um arquivo de script que define padrões de tráfego que simulam o funcionamento de uma aplicação UDP/IP *unicast* e/ou *multicast*, de forma periódica ou através de uma função de *Poisson*. Também é possível estabelecer a taxa de transmissão de pacotes por segundo e o tempo que irá durar a geração de tráfego. As estatísticas obtidas a partir da geração de tráfego pelo *Mgen* e de sua subsequente recepção pelo *drec* podem ser visualizadas de duas formas: em modo texto ou modo gráfico. Em modo texto, deve-se executar o utilitário *mcalc* para a geração de um relatório com as estatísticas do tráfego recebido, separado por fluxo e com um sumário de todos os fluxos transmitidos. Nessa estatística são exibidas informações sobre a identificação, a origem e o destino do fluxo, a quantidade de pacotes recebidos, a taxa de pacotes e dados recebidos, as taxas média, máxima e mínima do atraso, a variação do atraso e o número de pacotes descartados. Para a visualização gráfica do tráfego, devem ser utilizados o script *EZ* e a ferramenta *gnuplot*. O gráfico gerado dessa forma exhibe as taxas médias de pacotes, de bits e de atraso [18].

A Figura 8 - a seguir representa um script típico de uma configuração de tráfegos gerados a partir do MGEN. A Figura 8 simula, ainda, a geração de três tipos de tráfegos diferentes (Voz, vídeo, e dados), sendo que o tráfego de voz atende as recomendações do codec G711.



```

Sessão Editar Ver Favoritos Configurações Ajuda
# Autor: Eloy Tavares
# Trafego01_a_CPE02

START NOW
PORT 6000
INTERFACE eth0
TTL 10

# time flowid ON addr:port pattern rate size [RSUP ???] [TOS XX]

# Fluxo 1: voz - CODEC G.711
00000 1 ON 10.20.0.2:5000 PERIODIC 20.0 160 #consome em BW(Banda)=25,6kbps
#00000 1 ON 10.20.0.2:5000 PERIODIC 500.0 700

# Fluxo 2: video
00000 2 ON 10.20.0.2:5001 PERIODIC 30.0 400 #consome em BW=96kbps

# Fluxo 3: dados
00000 3 ON 10.20.0.2:5002 PERIODIC 50.0 500 #BW=200kbps; Pkts=500;T=10s
#00000 3 ON 10.20.0.2:5000 PERIODIC 20.0 4000

10000 1 OFF
10000 2 OFF
10000 3 OFF

# o caracter "#" significa comentario para aquela linha

# Example line to set IP header TOS bits to a given value (Linux, FreeBSD & NetBSD)
#00000 1 ON 132.250.95.23:5000 PERIODIC 10.0 128 TOS 24

```

Figura 8 - Script Exemplo - MGEN (Trafego01_a_CPE02)

De acordo com a Figura 8 é deduzida as seguintes interpretações para o primeiro tráfego:

Exemplificando o Fluxo 1 – voz CODEC G.711

- **00000** → Tempo de início de geração de pacotes;
- **1 ou 0001** → ID (Identificação);
- **ON 10.20.0.2: 5000** → Endereço para onde o tráfego é gerado: porta que será recebido.
- **PERIODIC** → taxa de reprodução periódica;
- **20,0 | 160** → Taxa de pacotes por segundos (*pps*) | Tamanho de *payload*.

OBS - 01: O caractere “#” significa que tudo seguido dele é um comentário.

OBS - 02: Os pacotes gerados são transportados usando o protocolo UDP - padrão do MGEN.

3.1.1.1 - Sintaxe básica do MGEN

Conforme anteriormente dito, as três sintaxes básicas do MGEN são os executáveis a seguir: - *mgen*; *drec* e, *mcalc* responsáveis por gerar, receber e ver estatísticas das aplicações, respectivamente. Os scripts seguintes representam a estrutura de cada uma dessas sintaxes.

SINTAXE DE GERAÇÃO DE TRÁFEGO:

“/usr/local/MGEN/”. /mgen /Trafego01_a _CPE02

Sendo que:

/mgen - É o executável que gera o tráfego a partir do script criado;

Trafego01_a _CPE02 – É o nome do script criado que contem a configuração dos tráfegos.

SINTAXE DE RECEPÇÃO DO TRÁFEGO (Iniciado antes do *script* de geração ser iniciado)

- **/usr/local/MGEN/drec -b ipaddr -i eth0 -S hora -d duração -p porta-porta**
“NomeArquivoaSeremGerado”

Sendo que:

-b = endereço IP da máquina que irá gerar o tráfego;

-i = nome da interface onde o tráfego gerado pelo mgen irá ser recebido;

-S = hora em que o programa drec irá iniciar a recepção de tráfego;

-d = duração da recepção de tráfego em segundos; e,

-p = número das portas que irão receber o tráfego gerado pelo mgen – arquivo:

“NomeArquivoSeremGerado” = **Trafego01_a_CPE02**

Para visualizar a estatística com detalhes de cálculo do *delay*, *jitter* e perdas, pacotes transmitidos, período de transmissão, estado de interface, quadros transmitidos, erro de transmissão e taxa média de pacotes transmitidos por segundos, é usado o comando **mcalc**.

Para vários fluxos concorrentes ao mesmo destino, “NomesArquivoSeremGerados” e portas devem ser diferentes.

SINTAXE DE EXIBIÇÃO DE ESTATÍSTICAS

“/usr/local/MGEN”. /mcalc Fluxo01_Trafego01_a_CPE02

Este comando deve ser executado depois do comando **drec** ter sido iniciado do lado do receptor.

3.1.1.2 -Classificação dos pacotes através do script MGEN

O gerador - MGEN permite classificar os fluxos através das marcações de alguns campos do cabeçalho, de acordo com os respectivos graus de precedência.

O MGEN e outros analisadores proprietários utilizados nos testes, mostraram todos os detalhes de QoS dos tráfegos e seus respectivos fluxos. Os parâmetros destacados são: Delay, jitter, perda de pacotes, além do tamanho do pacote os endereços de origem e de destino e as portas alocadas, o tamanho de *payload*, os bytes de cabeçalho e os protocolos utilizados. Segue o exemplo de uma classificação através do script MGEN com base na Tabela 5 - a seguir :

<p>• # Fluxo 1: voz - CODEC G.729</p> <p>00000 1 ON 10.20.0.2:5000 PERIODIC 20.0 160 TOS = 176</p>
--

Tabela 5 - Exemplo de classificação de tráfego a partir do script MGEN.

O exemplo do *script* da Tabela - 5, mostra a classificação de um tráfego prioritário através da marcação do bit do campo ToS = 176 do cabeça IP. O valor decimal 176 é equivalente ao somatório de 160 e 16 que indicam, respectivamente, o bit de Precedência e o de ToS. O valor 160 quer dizer tráfego com prioridade máxima (ECP-CRITICA) e o valor 16 tráfego com um baixo delay. São essas as principais

considerações sobre o MGEN e, na sequência, são apresentadas algumas características do analisador de tráfego e protocolo - Acterna - também utilizado durante os testes.

3.2 - ACTERNA EXAMINE DA3600 - *DATA NETWORK ANALYZER*

O Examine Acterna DA3600 é uma ferramenta de análise de tráfegos em redes e solução de problemas em rede IP avançada, baseada em *Hardware* e *software*. O Acterna é também utilizado para análise dos problemas em redes de pacotes sobre SONET/SDH (*Synchronous Optical Network / Synchronous Digital Hierarchy*). O Acterna é uma plataforma baseada em *hardware* e o Examine é um dos seus analisadores de protocolos baseados em plataforma de *software*. O proprietário é o *Acterna Inc.* O Acterna foi usado intensivamente durante praticamente todas as medições realizadas.

O DA-3600 realiza a análise de dados IP, solução de problemas e permite a interoperabilidade, testes de tráfego de pacote sobre as redes SONET, tanto em laboratórios como em ambientes operacionais. Ele fornece uma visibilidade sem precedentes em Fluxos de tráfego IP, com um desempenho até a taxa STM-16 linha (*Synchronous Transport Module*). O DA-3600 permite classificação dos fluxos e acompanhamento em tempo real de até 160.000 fluxos; permite, ainda, o acesso remoto em tempo real e mecanismo de classificação de fluxo com monitoramento de fluxo e solução de problemas, permitindo que seja reduzida significativamente, a *mean time to understand* - MTTU da origem dos problemas e, posteriormente, reduzir o tempo médio de reparo (*mean time to repair*) – MTTR [36]. O DA-3600 fornece uma série de características especiais:

- ✓ Suporte de monitoramento a 160.000 fluxos em tráfegos de rede;
- ✓ Monitoramento da rede em tempo real;
- ✓ Descodificação dos protocolos BGP, OSPF, IS-IS, e RSVP;
- ✓ Operações compatíveis com redes MPLS, incluindo mapeamento de redes IP a MPLS;
- ✓ Capacidade de acesso e controle remoto a dispositivos de teste geograficamente dispersos;
- ✓ Suporte a TCPDUMP, suporte NTP (*Network Time Protocol*), etc... [36].

3.2.1 - Características principais do Acterna.

O DA-3600 permite a criação de fluxos de definições personalizadas que determinam o tipo de fluxos a monitorar. Este processo é conhecido como classificação de fluxo, coleta e exibe estatísticas com base nos parâmetros de definição de fluxos anteriormente definidos na configuração dos roteadores. Esses parâmetros incluem rótulos MPLS, IP, Frame Relay, Ethernet, endereços de destino e origem, números de porta TCP / UDP, bits *flag* TCP, *Jitter* por fluxo, entre outras características em software.

Já na sua estrutura em hardware, os painéis são [36],[23]:

- ✓ Linha de *slots* interface - 1;
- ✓ Painel frontal com conectores RJ-45 10/100 Ethernet;
- ✓ Painel frontal com indicadores *Power*, *link*, erro;
- ✓ Painel frontal – LCD (*Liquid Crystal Display*) com instalação do dispositivo de teste;
- ✓ Controles do painel frontal do teclado *Setup*;
- ✓ Ethernet *crossover switch*
- ✓ Ligações na parte traseira DB-9 (GPS - *Global Positioning System*); GPS (CLK), GPS (PPS); GPS (CLK-O, PPS-O);
- ✓ Trigger (T-in, T-out);
- ✓ Slots painel traseiro Interface módulo *cardbus* dupla;
- ✓ Painel lateral Chave liga / desliga de energia.

3.2.2 - Identificar e medir a qualidade de serviço (QoS).

Existem muitas variáveis que afetam a qualidade do serviço na entrega de dados. Atraso do pacote, por exemplo, pode ser introduzido pelos roteadores, o número de saltos entre roteadores e congestionamento na rede, etc. Jitter excessivo também é comum afetar a qualidade do serviço de acordo com a aplicação tornando-se um problema para aplicações sensíveis ao atraso. Estes requerem um determinado tratamento do nível de QoS.

O DA-3600 identifica e isola latência de pacote por pacote através do monitoramento de jitter usando dispositivos de teste de um ou múltiplos presentes na rede. Essa característica de provisão de QoS é especialmente útil em rastrear a diferença no tempo de chegada de pacotes ou entrando ou saindo da rede como aplicações CBR

(*Constant Bit Rate*) orientadas a voz / áudio *streaming*, calculando através do parâmetro DeltaTime a média do jitter dos fluxos dos pacotes [36].

3.2.3 - Os benefícios do Acterna

Em redes operacionais de engenharia e solução de problemas os grupos de segurança, conta com os seguintes benefícios:

- ✓ Avalia os dados e faz inteligente balanceamento de carga, a fim de tráfego mal comportado não prejudicar o atual desempenho dos dados;
- ✓ *Downtime* de rede de forma proativa, com monitoramento para detecção de intrusão e negação de serviço - *Denial-of-service* (DoS).
- ✓ Verificação dos protocolos de roteamento de interação (BGP, OSPF, IS-IS) com foco em monitoramento em tempo real de controle de mensagens para a realização de interoperabilidade entre os equipamentos de testes;
- ✓ Verifica a operação das redes IP/MPLS em *real time* verificando o mapeamento dos *labels* para garantir a adesão do elemento de roteamento com as especificações e configurações mais adequadas [36].

3.2.4 - Roteamento em tempo real e sinalização dos protocolos de monitoramento.

O DA-3600 monitora em tempo real os protocolos de roteamento e a atividade para OSPF, IS-IS e BGP-4. Além disso, os protocolos de sinalização e suas respectivas mensagens como RSVP, CR-LDP e TDP são controlados em tempo real.

A contagem de todas as mensagens dos protocolos é exibida, permitindo ver o *status* de todos os protocolos. Informações de protocolos e evento de sinalização dos protocolos são a qualquer momento decodificados e exibidos em profundidade da informação que podem ser visualizadas clicando no evento em questão [36].

3.2.5 - Estatísticas de fluxo em tempo real em Acterna

As estatísticas sobre todos os fluxos de entrada são APRENDIDAS, combinando os parâmetros situados no *FlowClassifier*. As estatísticas incluem a utilização de taxa de pacotes, taxas de pico, jitter médio, protocolos utilizados, endereços usados, portas usadas, tipo de codec, etc... [23].

3.2.6 - Transmissão em Acterna

A linha de funcionalidade da taxa de transmissão está disponível em até OC-48c/STM-16. É possível criar vários tipos de pacotes, incluindo (PPP, IP, TCP, MPLS multicast e unicast) para a transmissão em ambos os payload com tipos de cabeçalho especificado individualmente. O número de pacotes transmitidos é limitado pelo buffer de transmissão de 64Mb [36].

O Capítulo IV a seguir diz respeito à parte dos testes de laboratório a serem realizados. Para tal é definida toda a metodologia necessária para determinar os testes, desde descrição e organização do laboratório ao tipo de testes, assim como a definição de alguns parâmetros julgados úteis para realização dos testes e a especificação do software gerador de tráfego [23].

4 - CAPÍTULO IV: ESPECIFICAÇÃO DOS TESTES E, CENÁRIO DE TESTE.

*“Mesma as noites totalmente sem estrelas podem anunciar
a aurora de uma grande realização”
– Martin Luther King Jr*

Justifica-se a necessidade deste capítulo por razões de natureza técnica e organizacional, uma vez que a realização dos testes para chegar ao objetivo desta dissertação, requer entendimento de questões do tipo infraestruturais ligadas a limitação de recursos presentes no laboratório como é o caso da carência de banda. É necessário, contudo, especificar os testes a fim de que seja seguida uma ordem lógica dos testes que ajude, portanto, a entender e comparar os resultados dos diferentes analisadores de protocolos usados, dentro da perspectiva da provisão de Serviços VoIP em *link* de banda estreita compartilhada. Ademais, torna-se importante entender também a estrutura do cenário laboratorial físico disponibilizado e como este foi adaptado para que fossem realizados os testes. As figuras que representam as duas topologias são ilustradas na próxima seção – subseção: “*Cenário dos testes de medições*”.

4.1 - Especificação dos Testes Laboratoriais:

Os resultados para os testes laboratoriais seguem especificados conforme descrito a seguir. No entanto, quase todos os testes implicaram na geração de tráfegos usando o MGEN, tendo sido, também, medidos pelo MGEN e o Acterna, comparativamente. Os tráfegos gerados passaram obrigatoriamente pelo Backbone – IP/VPN MPLS Multicast conforme ilustra inicialmente a Figura-9 da Seção 4.2 a seguir a esta seção (4.1) e as respectivas Sub-Seções. A Seção 4.2 - *Cenário dos testes de medições* - detalha com riqueza de informação as questões relacionadas a topologia da rede. Esses tráfegos Multicast ou Unicast, partiram de um dos geradores (GER01, ou GER02 ou GER03) e posteriormente por um dos roteadores denominados CPE's que fazem conexão *Fast-Ethernet* com os geradores (GERxy), conforme a Figura-10 da Sub-Seção - 4.2.2 mas adiante. Estes CPE's estão conectados de um lado com os clientes e de outro lado fazem conexão serial com os roteadores de bordas do Backbone. As especificações dos testes, seguem enumeradas:

4.1.1 - O que testar e quais testes fazer

Pretende-se testar a viabilidade dos serviços VoIP em links de baixa capacidade, onde haja compartilhamento de outros serviços - tipo transmissão de dados FTP, videoconferência - sobre o mesmo enlace Frame Relay de 512kbps. Dados estes requisitos em pauta, tornou-se necessário testar em enlace Frame Relay tecnologia de acesso disponível na ocasião e, posteriormente, serão também analisados opcionalmente os protocolos nível do Backbone MPLS. Vale realçar que os testes incidirão essencialmente sobre o padrão FRF.12, recomendado pelo Frame Relay, uma vez que este (FRF.12) possui recursos necessários que permitem testar e chegar ao objetivo pretendido. Com isso pretende-se realizar testes onde são analisados a eficiência e a eficácia do FRF.12 e é também medida a ocupação da banda quando for habilitada a cRTP ou quando não for habilitada a cRTP. Parâmetros como jitter, atraso, adequação dos codecs as aplicações de voz, percentual de perda de pacotes, etc..., são igualmente medidos.

(1) - Com relação à banda passante, o total de 512kbps de link L2 da tecnologia de acesso Frame Relay – Recomendação FRF.12, é distribuído de acordo com as classes de tráfegos da seguinte forma:

- 400kbps reservados a aplicação de Dados e multimídia;
- 60kbps reservados a aplicação de tempo real (Voz);
- 52kbps destinados ao tráfego default - aos demais tráfegos de tipo *ftp* (Dados comuns sem qualquer política de prioridade);

OBS: Notas explicativas sobre a partilha dos 512kbps de banda:

NOTA 01: Pretende-se testar a transmissão de voz em links de 512kbps que trafegam dados, porém, com consumo mínimo possível de voz, sendo assim para codec G729 são 60kbps.

NOTA 02: A banda reservada para classe voz e *default*, varia de acordo com o codec a ser utilizado. Cada codec requer um limite mínimo de banda para cada canal de voz em um enlace Frame Relay com / sem compressão de cabeçalho. A especificação anterior (60kbps) atende ao codec G729 e a reserva de 52kbps é para classe *default*, ou seja, essa classe (*default*) recebe a diferença da soma da classe voz

e *business* em relação ao total de 512kbps; se, no entanto, tivesse sido usado outro codec como o G711 - que requer mais banda acima de 60kbps e 400kbps para a classe *business* - logo a classe *default*, teria recebido o restante da banda dos 512kbps. Logo, a banda reservada para classe *default* seria nesse caso inferior a 52kbps;

NOTA 03: A maioria dos testes foi realizada usando o codec G729, pelo fato da operadora usar essa configuração como sendo um perfil de tráfego para a rede de voz deles projetado;

NOTA 04: Os 60kbps foram uma parcela de banda reservada para aplicação de voz usando codec G729, pois é recomendado, pelos fabricantes de equipamentos de comutação, reservar para esse codec 31.2kbps para link ethernet; 26.8kbps para link FRF.12 sem compressão e, 11.8kbps, para enlace FRF12 com compressão [5]. Dessa linha foi reservada 60kbps, que inclui também uma folga de mais de 45% sobre quaisquer recomendações para tráfego de voz usando G729.

NOTA 05: Foi necessário reservar o mínimo de banda aconselhável a voz, pois o PVC é de transmissão de dados e quer-se apenas testar como comporta a voz em paralelo, neste enlace;

NOTA -06: A classe *business* (*Dados e videoconferência*) precisa de ter em média os 78.13% de banda, pois os tráfegos de dados e videoconferência são normalmente volumosos, acima de 1500bytes. Ademais o PVC é dedicado para estes tipos de transportes [5],[37].

(2) - Medições comparativas da viabilidade dos codecs (G711, G723, G726 e G729) em equipamentos de plataformas diferentes CISCO, HP3800, MX-One e o software Asterisk, usando um telefone analógico. Esses testes foram executados com o objetivo de decidir quais dos codecs são melhor indicados para trabalhar com voz em plataforma cisco e a sua tolerância a perda [37];

(3) – Testes de validação do gerador de trafego / receptor de tráfego – MGEN comparativamente com o simulador de rede *WAN* o analisador Acterna; Essas bancadas

de testes que seguem especificadas nos itens 3.1 e 3.2, visaram validar o gerador MGEN em relação aos geradores proprietários em uso pela operadora. Pois, o MGEN fora assim usado pela primeira vez em testes de tal dimensão, precisava assim ser testada a sua confiabilidade:

(3.1) – Medições com tráfegos simples, pequenos e sem fragmentação avaliando a rede e comprovar os testes 3, partindo de um dos geradores anteriormente citados com destino ao Ger02 passando por CPE02;

(3.2) – Medições de perda, jitter, pacotes enviados e recebidos, etc, usando ferramentas MGEN para gerar, coletar e analisar os resultados de acordo com as políticas de QoS setadas na modelagem e controle de tráfego segundo o Modelo FRTS (*Frame Relay Traffic Shaping*);

(4) – Medições sem quaisquer políticas de QoS (nos roteadores e gerador) e sem fragmentação de pacotes de dados disputando a fila com fluxos de *frame* de voz RTP usando Codec G729 e ramais telefônicos com conversa em tempo real e sem compressão de RTP. Este tipo de teste, visa analisar o valor de atraso, jitter, ocupação da banda, qualidade da voz e taxa de perda;

(5) - Medições com QoS nos CPE's e Backbone e com fragmentação interleaving (LFI) habilitada a 640 bytes, respeitando as políticas de QoS, usando as conexões Frame Relay DTE – DCE e pacotes voz de payload 160bytes usando o codec G711 com transporte UDP. Com os testes especificados nos itens 5.1, 5.2 e 5.3, pretendeu-se testar o comportamento de pacotes de voz intercalados entre os pacotes de dados e analisar a sua viabilidade com aplicação de QoS e sem a aplicação de QoS, com a compressão e sem a compressão:

(5.1) – Repetição de Medições 5 - usando telefones Ramais 3000 e 5000 com conversação em tempo real com QoS e sem QoS;

(5.2) – Repetição dos testes 5 não respeitando as políticas de QoS negociadas;

(5.3) – Medição idem ao item 5, contudo, usando o codec G729 – frame de voz de 66 bytes sem compressão com prioridade máxima sobre os tráfegos FTP de 1000 bytes;

(6) – Medição de LFI usando o G729 com QoS a nível do GERADOR – MGEN classificando e priorizando o tráfego de voz no próprio *script* do MGEN com análise

dos tráfegos a serem marcados nos *scripts* dos CPE's: Estes têm como objetivo validar a aplicação com QoS a partir do gerador MGEN, ao invés da configuração nos Roteadores e análise da sua confiabilidade;

(7) - Medições de compressão de cabeçalho RTP (cRTP) habilitada na interface, utilizando o codec G729 com VAD desabilitado com transmissão de voz em tempo real, usando os ramais 3000 e 4000 para CPE02 e os ramais 5000 e 6000 para o CPE03, com tráfegos de apenas um fluxo de voz passando pelo Backbone. Esses testes, de acordo com os itens 7.1 e 7.2 têm como objetivo analisar a viabilidade de tráfego *multicast* quando aplicado a QoS e sem a QoS onde dois canais de voz são habilitados para conversação simultânea entre quatro pessoas:

(7.1) – Repetição do teste do item 7, mas com dois fluxos de voz em paralelo com duração de 8 minutos cada, a fim de analisar a ocupação da banda, a compressão de cabeçalho, o atraso e a viabilidade das aplicações e quantidade de pacotes gerados;

(7.2) – Repetição do teste item 7 com compressão desabilitada no acesso Frame Relay;

(8) – Os testes desta seção, objetivam analisar os parâmetros de QoS e MPLS dos fluxos de voz no backbone IP/MPLS, testando apenas um fluxo de voz e sem compressão;

(8.1) – Repetição do teste do item 8, com dois fluxos de voz em paralelo e com compressão de RTP e análise também do protocolo CRTP;

(9) - Testes complementares com LFI habilitado envolvendo diferentes Codec como G711, G726 e G729, com compressão de cabeçalho e sem compressão de cabeçalho, com QoS e sem QoS e com plotagem de gráficos comparativos, tendo como objetivo analisar a banda ocupada na rede, jitter das aplicações, verificar a intercalação dos pacotes entre os fragmentos de 640bytes e 540bytes, o tamanho de pacotes quando ocorrer a compressão RTP e a viabilidade do VoIP:

(9.1) - De acordo com o item 9, são medidas aplicações num primeiro momento sem quaisquer políticas de QoS, sem cRTP, sem LFI, testadas com os três codecs diferentes conforme item 9;

(9.2) – Num segundo momento, de acordo com o item 9, são medidas aplicações com políticas QoS configuradas, cRTP desabilitada, com LFI a 640bytes e testadas com os três diferentes codecs;

(9.3) – Já num terceiro momento, são testadas aplicações com políticas QoS, com cRTP habilitado na interface serial, com o LFI a 540bytes e testadas, igualmente, com os três diferentes codecs;

(9.4) – Em um quarto momento, são medidos o comportamento da rede e as aplicações perante 1 (um) Fluxo de real time (Voz) usando o codec G729 e 2 (dois) tráfegos FTP concorrentes, sendo cada fluxo de 1000 bytes de payload a uma reprodução periódica de 10sec a 30pps. Entretanto foi habilitada a compressão de cabeçalho e os fragmentos gerados são de, no máximo, 540bytes.

Uma vez especificados os testes, torna-se interessante especificar o cenário dos testes, incluindo a topologia da rede projetada para tal fim. A seção 4.2 a seguir trata disso.

4.2 -Cenário dos testes de medições

O cenário dos testes resume-se conforme a topologia inicial - Figura 9 - a seguir, projetada para fins de teste VoIP em redes de pacotes. Esta topologia diz respeito a uma topologia física inicialmente implementada e que veio a sofrer readaptações lógicas e físicas, conforme ilustrada mais adiante na Figura 10.

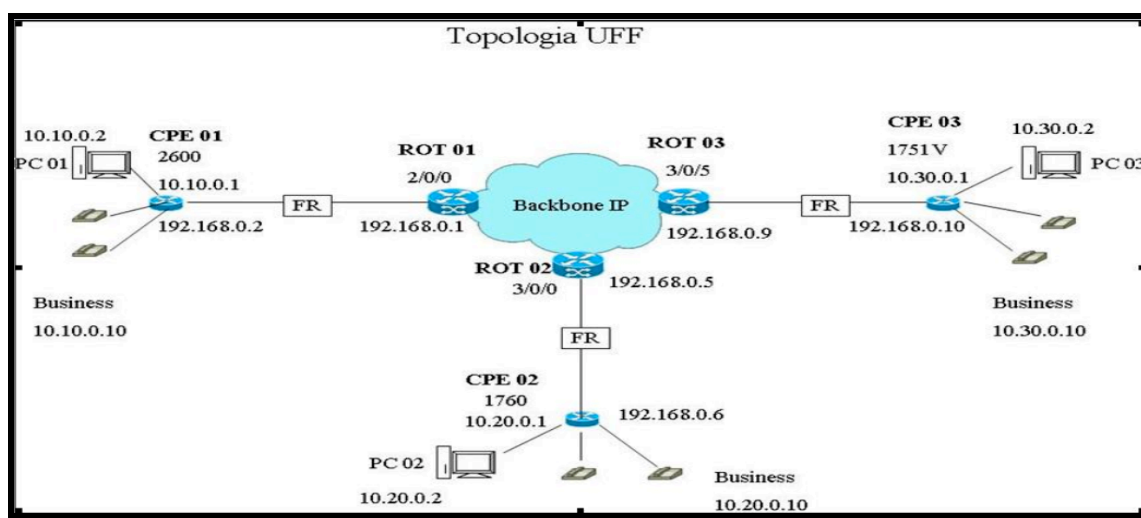


Figura 9 - Topologia Física – Inicial.

A Figura 9 representa o ambiente topológico inicialmente estruturado e disponibilizado para testes de serviços VoIP, IPTV, em enlaces compartilhados de

512kbps que trafegam dados do tipo FTP, denominados pela operadora como sendo classe *Business*.

Todos os testes realizada da OP seguiram, igualmente, os princípios tecnológicos IP/VPN/MPLS. Com relação aos softwares, anteriormente, o laboratório era equipado com Acterna Examine, Wankiller, Smartbits e eram usadas apenas máquinas Windows 2000, visto que pois os analisadores eram baseados unicamente em plataforma Windows.

4.2.1 - Os equipamentos de comutação presentes no laboratório.

Analisando a Figura 9 ou a Figura 10, percebe-se, também, que a rede é composta por pelo menos seis (6) roteadores, sendo 3 (três) de borda do backbone IP/VPN/MPLS e 3 (três) roteadores de acesso aos clientes. Desses equipamentos pode-se afirmar que:

- ✓ Os roteadores de borda são denominados de ROT com os seus respectivos endereços IP e *interface* serial: ROT01: (192.168.0.1: 2/0/0); ROT02: (192.168.0.5: 3/0/0) e o ROT03: (192.168.0.9: 3/0/5) esses equipamentos são todos do fabricante Cisco;
- ✓ Os equipamentos de acesso, chamados de Roteadores - CPE (*Customer Premise Equipment*) são identificados pelos IP: CPE01 (192.168.0.2); CPE02 (192.168.0.6); CPE (192.168.0.10);
- ✓ Os ROTs e os CPE's se conectam através de um link frame Relay de 512kbps entre si;
- ✓ Os CPE's são equipamentos com *interfaces* seriais e *Ethernet*. As interfaces seriais por um lado, provêm acesso aos ROTs enquanto que as *interfaces Ethernet*, por outro lado, provêm acesso aos equipamentos dos clientes;
- ✓ Todos os equipamentos CPEs trafegam tráfegos *unicasting* e ou *multicasting*. Estes tráfegos partem de uma estação geradora de tráfego e entregam para uma estação, ou para duas estações receptoras simultaneamente;
- ✓ Os roteadores que compõem o laboratório são de plataforma Cisco modelos – 2600, 1760, 1751; Esses equipamentos são dotados de algumas funções

indicadas a seguir que os permita dar suporte de forma cabal aos testes realizados; as funções em causa são:

- Capacidade Canal -Suporta de 30 a 48 canais de voz [38],[40];
 - Arquitetura DSP (*Digital Signal Processor*) flexível permitindo seleccionar o codec adequado de forma dinâmica quando uma chamada é estabelecida, embora o administrador de rede possa fazê-lo;
 - São utilizadas as seguintes portas de *interfaces* de voz de suporte a FXS, FXO, DID, E/M, BRI (S/T, NT/T), T1 e E1. (T1 e E1 apenas suportado em NM-HD-2VE), serial, Ethernet, RJ-45 [39] [42];
 - Permitem mecanismo de compressão de alto desempenho - oferecendo um desempenho de compressão de velocidades de até 64 vezes do que soluções baseadas em software [41];
 - Para transportar voz sobre redes de pacotes, estes permitem as técnicas [39]:
- 1) Voz / fax sobre IP- Tráfego VoIP na camada 3 (L3), podem passar por qualquer outras camadas L1 ou L2, incluindo ISDN, linhas sob concessão, permitem conexões seriais e Ethernet;
 - 2) Oferece compressão RTP e técnicas de fragmentação de pacotes que permitem a qualidade de voz e transmissões de fax através de qualquer conexão WAN;
 - 3) Controle de Admissão de chamadas e *Fallback PSTN* usam *Service Assurance Agent* (SAA) para determinar atraso de latência, jitter e fornecer em tempo real cálculos - *Calculated Planning Impairment Factor* (ICPIF) antes de estabelecer uma chamada através de uma infraestrutura IP. Os SAA permitem que pacotes de voz recebam a mesma prioridade em toda a rede;
 - 4) Mecanismo de QoS avançado é configurável. A QoS em Cisco IOS *Software* permite manipular características de reserva de largura de banda adequada e priorizar tráfego de voz e fax para ajudar a garantir a entrega transparente de qualidade de voz e fax. Estes

equipamentos incluem ainda protocolos RSVP, técnicas enfileiramento como LLQ, Precedência IP, serviços *diffserv* baseados em campos DSCPs [22];

- Interopera fim-a-fim com telefones IP, telefones analógicos, com conexões de fax, e conexões PBX ou PABX ou com outros produtos habilitados para conexão de voz implementados em equipamentos de plataforma cisco;

Os usuários podem optar por transmitir a voz em suas redes usando os codecs como PCM sem compressão (G.711, μ -law e A-law) ou comprimido de 5,3 kbps a 32 kbps ou utilizando codecs cujos algoritmos são baseados em padrões de compressão (G.729, G.729 / b , G723, G.723.1, G.726, G.728) [40];

- Transmitir a voz sobre IP através de um Frame relay, ATM, ISDN,MLPPP[40];

Suporte a VoIP, VoFR e apoio VoATM (*Voice Over ATM*); recursos do H.323, H.323 com negociação de CODEC; Suporta ao Padrão ITU com algoritmos de compressão (G.729A, G.729B, G.711a e μ -law, G.726 todas as versões, canal de fax-relay, G.728, G.729, G.729B, G.723a G.723 e todas as restantes versões, GSM (*Global System for Mobile Communications*) GSMEFR (*GSM Enhanced Full Rate*),VLAN,VPN,VPLS e relé modem [40];

- Aloca largura de banda com prioridade para aplicações nas interfaces WAN com melhor desempenho usando as seguintes técnicas: CAR, políticas de roteamento, WFQ, LLQ (também chamado de (PQ/CBWFQ), WRED, GTS, DSCP, FRF.12, FRTS,cRTP, RSVP + H.323v2 [38].

Essas são algumas das mais importantes características dos equipamentos de comutação presentes no laboratório e que foram de fato usados durante todos os testes.

4.2.2 - Readaptação da topologia física em lógica

A topologia lógica segue todos os princípios descritos na topologia física. Assim, de forma análoga a topologia física inicial, conforme ilustrada na Figura 10 a seguir, fica composta por estações geradores e receptores de tráfegos (Ger01,02 e 03), ditos, respectivamente, de estações PC01,02 e 03. Cada uma dessas estações possui mais de uma placa de interface Ethernet e equipados com OS (*Operating Systems* - Sistema Operacional - *Linux Slakware v11*). Há uma quarta estação conectada ao Acterna, de plataforma *Windows*, que roda o software do Acterna.

Essa topologia (lógica) readaptada - Figura 10, contrariamente à topologia inicialmente disponibilizada - Figura -9, usa na sua maioria máquinas Linux, visto que foram gerados tráfegos FTP, a partir do MGEN, apesar de haver também uma outra máquina Windows de suporte ao analisador Acterna. O acterna é um equipamento que fizera parte da estrutura inicial do laboratório. Entretanto, a grande diferença da topologia inicial da lógica, centra-se na estrutura de QoS e a utilização de vários outros tipos de codec como G711 e G726. É que, inicialmente, a rede fora projetada apenas com o codec G729.

O Acterna é um dos equipamentos proprietários do Nível dois (L2) que a OP usa nos seus laboratórios de teste. Esse equipamento captura e analisa os tráfegos que passam nas interfaces seriais que ligam o CPE (*Customer Premise Equipment*) 02 e ROT 02, sendo esse último equipamento também chamado de PE (*Premise Equipment*) 02. Este equipamento permitiu visualizar a intercalação dos pacotes gerados e visualizar os demais parâmetros de tráfegos associados às aplicações, pois o MGEN embora gera, captura e analisa não mostra todos os detalhes como os do analisador Acterna. O Ger01 possui em particular três interfaces Ethernet eth0, eth1 e eth2 e as demais estações possuem apenas eth0 e eth1 e cada uma dessas interfaces aloca um endereço IP diferente. Por exemplo, o eth1 e eth2 são usados para os endereços de rede de gerência e eth0 para a rede de teste. A estação PC01 possui três interfaces ethernet por isso ela faz conexão com as demais estações e permite também acesso do PC02 a PC03 e vice-versa.

Para que os testes de medição fossem, efetivamente, realizados, usou-se apenas os endereços de operação do tipo como, por exemplo: 10.10.0.2 e ou 192.168.0.2 conforme ilustrada na topologia, uma vez que desses endereços temos acesso aos roteadores ditos de CPE's, ao PE's e, por conseguinte, ao Backbone. Admitindo-se que os testes ocorreram predominantemente a nível 2 (L2) e com a coleta de dados nas estações receptoras mas também nos roteadores onde estão todas as políticas de QoS e as tecnologias de enlace como o caso do FRF.12 (*Frame Relay Fórum 12*), torna-se inútil realizar teste que não seja pelos endereços de operação acima referido.

Os endereços de gerência (p.ex: 10.255.3.2) servem para as estações acessarem-se mutuamente e os dados transmitidos por esses endereços de gerência são ponto-a-ponto entre os hosts. Não passam, portanto pela interface serial nem por backbone. Convém frisar que a topologia a seguir, usada na realização dos testes é, além de tudo, um cenário de uso multifornecedor e compartilhado. Considerando esse cenário, os testes foram realizados tendo sempre em mente a manipulação conveniente de alguns dos parâmetros como, *p.ex.* a QoS, para não afetar, de forma degradante, toda a operação pela rede compartilhada na OP.

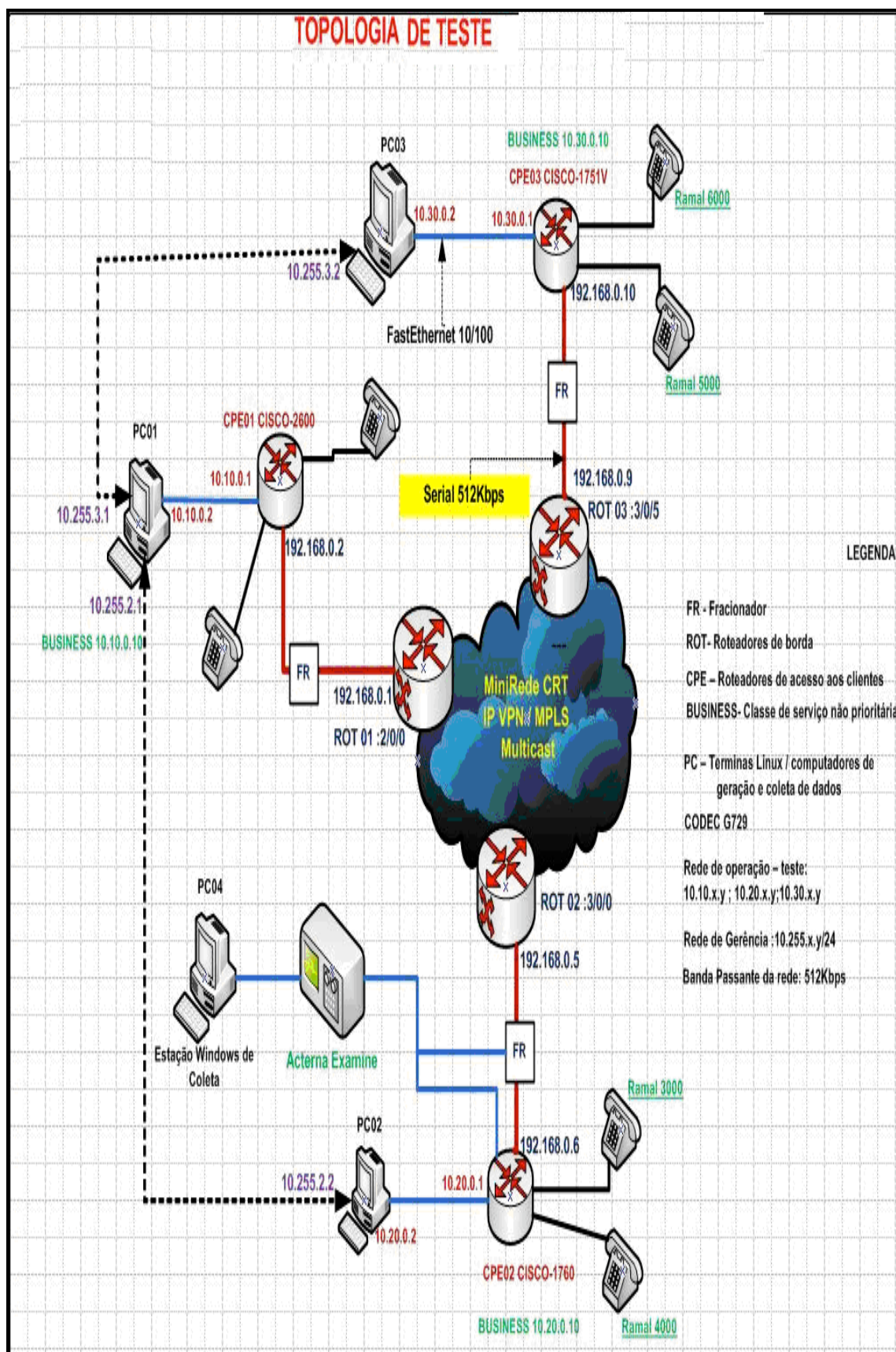


Figura 10 - Topologia lógica UFF – OP-Operadora de Telecomunicações

Em resumo nota-se que na Figura 10, tem-se no acesso ao backbone IP VPN /MPLS Multicast, três roteadores de borda denominados de ROT 01, ROT 02 e ROT 03, que formam, portanto, uma mini-rede de “três pernas”, ou seja, com três roteadores de acesso que através de uma interface serial de 512kbps ligam-se cada um deles a mais um roteador de acesso denominado de CPE que faz *interfaceamento* através do *link Fast/Ethernet* aos equipamentos secundários da rede que são operados pelos usuários como: ramais telefônicos, estações de trabalho que geram e recebem tráficos bem como o equipamento Acterna Inc.

Para a topologia da Figura 10 são adotados outros perfis de tráfego que compõem as políticas de QoS para os testes de avaliação de serviços VoIP em enlace compartilhado, conforme denotado no trecho de *script* da Tabela 6 - a seguir. Para os testes que compõem esta dissertação, foram criadas três classes de serviços (CoS) a saber: Classe *Business* (Dados), classe voz e classe *default*.

```

• policy-map FILA_QOS
•   class VOZ
•     set ip dscp ef
•     compress header ip rtp
•     priority 60
•   class BUSINESS
•     set ip dscp af31
•     bandwidth 400
•     random-detect dscp-based
•     class class-default
•     fair-queue
•   !
• map-class frame-relay FR_QOS
•   frame-relay cir 512000
•   frame-relay bc 6144 → quanto pode ser enviado por unidade de intervalo de tempo em bits BC(Tamanho de rajada)
•     frame-relay be 0
•     frame-relay mincir 512000
•     service-policy output FILA_QOS
•     frame-relay fragment 640
•   access-list 100 permit udp any eq 6000 any eq 5001
•   access-list 101 permit udp any eq 6000 any eq 5000
•   !

```

Tabela 6 - Definições de classes e modelagem FRTS configurado nos roteadores CPE da OP.

Na Tabela 6, percebe-se através da configuração do scrip, que o fragmento de datagramas foi setado para 640 bytes, CIR a 512000 bytes, BC a 6144bytes, banda de dados a 400kbps, fila *fair queue*, marcação AF31 e para a classe de voz teve a marcação ef, fila *priority queue*, e banda reservada a 60kbps.

As três CoS que foram definidas para os novos testes, receberam 400kbps, e 60kbps para CoS business e voz, respectivamente. Essas mesmas classes foram escalonadas com as seguintes filas: Strict priority para voz, fair queue para business e FIFO para classe default, tendo esta última classe recebendo sempre a diferença da banda total (512kbps) do somatório das duas classes de serviços. Ainda na Tabela 6 - Definições de classes e modelagem FRTS, além de nos mostrar as classes, mostra algumas políticas de modelagem FRTS de tráfego como os valores reservados para BE, BC, CIR, etc.

Após essas considerações, é plausível realizar a análise dos resultados observados durante todos os testes realizados. O Capítulo V - seguinte trata de resultados parciais, ou seja, dos primeiros resultados extraídos.

5 - CAPÍTULO V: RESULTADOS PARCIAIS - MEDIÇÕES LABORATORIAIS.

*“Há duas formas de viver sua vida; Uma é acreditar que não existe milagre
A outra é acreditar que todas as coisas são de milagre.”*

- Albert Einstein

Neste capítulo, são apresentados os resultados parciais, ou seja, os primeiros resultados extraídos dos testes realizados. Nesses testes, os parâmetros de melhoria de desempenho da rede como a cRTP, Codec, LFI, QoS, são testados em de medições independentes, sendo assim, estes testes parciais são os mais simples. São testes do tipo validação e comparação dos resultados a partir dos softwares de análise, avaliação dos codec em relação aos equipamentos e avaliação da fragmentação com intercalação, etc. Os testes em questão são abordados em seções, conforme seguem:

5.1 – Objetivos das medições parciais sobre a viabilidade dos codecs em relação aos equipamentos de diferentes plataformas.

Os testes de medições sobre os codecs que constam desta seção foram realizados também em outros trabalhos monográficos [37] com o objetivo de validar a adequação dos codecs de voz em alguns equipamentos de comutação e principalmente, a sua eficácia em equipamentos cisco a fim de validar quais deles são mais toleráveis à perda e que ao mesmo tempo apresenta mais adequação para os equipamentos cisco.

Com relação aos testes de Codecs, é medida a tolerância a perda de pacotes de alguns CODECs mais utilizados entre os quais foram testados CODECs [6] sem perda (G.711) e com perda (G.729 e G.723) e ao longo dos testes experimentais, é também utilizado o CODEC G.726. O outro objetivo desta seção de teste é avaliar a adequação dos codecs testados em relação aos equipamentos de comutação, a seguir discriminados. Os testes de codecs são assim realizados usando 4 (quatro) equipamentos diferentes, exercendo o papel do ATA (*Analogic Telephone Adapter*) – equipamento PABX. Estes quatros equipamentos são: roteadores CISCO 1751, MX-One; HP-3800¹⁸ e Asterisk.

¹⁸ Os equipamentos da plataforma MX-One e o HP-3800, não foram equipamentos disponíveis no laboratório da OP. Estes equipamentos foram disponibilizados pela FIRJAN. Ademais, estes testes de validação e análise dos codecs em relação aos equipamentos HP-3800, Mx-One, CISCO 1760 e Asterisk, foram realizados separadamente nas dependências da FIRJAN, os resultados observados segundo a Tabela 7, são de caráter complementares, uma vez que mais afrente outros estudos envolvendo codec são realizados, comprovando esses estudos preliminares sobre codecs [37].

5.1.1 - Porquê realizar estes testes

Esses testes são realizados com o intuito de avaliar quais dos codecs apresentam melhor desempenho em aplicações VoIP, sobre as diferentes plataformas de equipamentos de comutação. Feito isso fica mais fácil escolher o codec que melhor lida com aplicações VoIP em enlace de baixa capacidade.

5.1.2 - Critérios metodológicos para desenvolvimento desses testes

De acordo com os testes de avaliação dos codecs nos quatros equipamentos listados acima, são obtidos resultados específicos relacionando cada equipamento representado pelo ATA e, dessa forma, o equipamento ATA fora alternado fisicamente um de cada vez, para cada codec usado em função do uso dos seguintes equipamentos das plataformas:

- CISCO 1751; MX-One; HP-3800 e, Asterisk contendo o telefone analógico conectado a eles alternadamente, isto é, quando se queria testar o desempenho dos Codecs usando, por exemplo, o roteador CISCO desconectava-se o equipamento conectado ao Emulador WAN ao qual também estava conectado o telefone (por exemplo, podia ser um equipamento HP – 3800 que faz o papel de um ATA) e colocava-se no lugar deste equipamento desconectando um outro equipamento por exemplo, o roteador CISCO.

Em resumo, fases de testes com os diferentes equipamentos, ora ligava-se o telefone analógico a FXS (*Foreign eXchange Subscriber*) do roteador Cisco 1751; ora ligava-se o telefone ao PABX MX-One da Ericsson; ora ligava-se o telefone ao PABX HP3800 da Siemens; e ora ligava-se o telefone analógico a um Servidor Asterisk (Servidor de voz) que depois de configurado para um determinado Codec passava-se a realizar os testes específicos a cada plataforma.

O ATA representa os quatros diferentes equipamentos de testes que se queria testar os diferentes codecs para que os resultados adquiridos em cada equipamento específico viessem a ser comparados conforme mostra a tabela abaixo:

- Percentagem de perda de pacotes onde a voz se torna ininteligível. Desses telefones parte o diálogo que é analisado a partir da configuração de um emulador de

WAN para Linux chamado NETEM¹⁹ [17] (Emulador de WAN – do próprio Kernel do linux. O Cenário é representado conforme a Figura 11 - que se segue:



Figura 11 - Cenário de Implementação teste análise de CODECs [37]

Todas as ligações telefônicas foram feitas de um ramal telefônico, passando pelo Emulador de WAN ao Servidor de voz. Este atende a chamada e, automaticamente, dispara um arquivo de fluxo de áudio que inicia a reprodução de uma mensagem gravada onde uma pessoa lia um texto qualquer. Neste mesmo instante, o emulador de WAN entra em ação inserindo uma perda de pacotes controlada no caminho da voz fazendo com que a reprodução sofra perda aleatória crescente em degraus de 0,5%. Quando a voz começa a ficar ininteligível, o teste acaba.

O valor da perda tornava-se mais perceptível de acordo com o estado do congestionamento do buffer de recepção à medida que o tempo passava. O teste foi repetido com várias pessoas e o valor final representa uma média dos valores individuais [37].

5.1.3 – Resultado - Matriz – correlacionando codecs e os equipamentos de testes

A Tabela 7 - a seguir ilustra os resultados desse teste, em que os equipamentos são testados em mesmas condições de carga, o equipamento Asterisk foi também testado com o G729b, pois a OP (Operadora de Telecomunicações) possui o licenciamento do uso; ademais todos os testes realizados usando o codec G729 são baseados na extensão – anexo “b” que dá suporte ao VAD – *Detect Voice Activity* possui o módulo DTX (*Discontinuous Transmission*) e ao módulo do decodificador CNG (*Confort Noise Generator*), conforme explicado na seção de teoria.

¹⁹

O emulador de WAN e o Servidor de Voz foram instalados na mesma máquina Linux.

CODEC	CISCO	MX-One	HP-3800	Asterisk
G711 (ulaw)	41,5	25	43,5	28
G729 (b)	32	21,5	39,5	27
G723.1(6.3kbps)	27	18,5	25,5	23
G726 (32kbps)	42	NA	NA	29

Tabela 7 - Porcentagem de tolerância a perda de pacotes por codecs de voz [37]

Nota-se, portanto, que os equipamentos Siemens HP-3800 e Cisco 1751, usando todos os CODECs, apresentaram maior tolerância a perda de pacotes quando comparado os demais equipamentos. Isto se deve ao fato deles utilizarem algoritmos que substituem uma porção da voz perdida por uma estimativa calculada do que seria aquele fragmento. Usando o equipamento CISCO e o CODEC G.726, obteve-se o segundo melhor resultado com uma tolerância de 42,0%. O teste com a plataforma HP-3800, não teve sucesso.

5.1.4 – Interpretação dos resultados parciais dos testes de CODEC

Concluiu-se que, em média, a melhor plataforma foi o CISCO cujos resultados da tolerância a perda, mantendo a boa audibilidade a altas taxas de perda apresentaram os seguintes valores para os CODECs: G.711 μ -law – 41.50%; G.729 – 32,00%; G.723 (6,3Kbps) – 27,00% e, G.726 (3.2Kbps) – 42,00%. Dos resultados dos testes conclui-se, ainda, que os CODECs G711 e G726 são mais tolerantes a perda de pacotes. O CODEC G729 vem em seguida com boa tolerância a perda. Por último, o G723 é o menos tolerante a perda de pacotes. Observe que o roteador Cisco e o PABX Siemens apresentam maiores valores para tolerância a perda de pacotes. Isto se deve ao fato desses equipamentos possuírem um mecanismo que amenize os efeitos da perda de pacotes, estimando um valor para os pacotes perdidos [37].

5.2 - Testes preliminares sobre a QoS e LFI

Os testes preliminares, ou testes parciais, são considerados os primeiros testes realizados, onde poucos parâmetros são manipulados. Neste caso, são manipulados os parâmetros de melhoria de desempenho como a QoS e LFI, usando o codec G711. Serão também medidos os parâmetros como o Jitter, perda, consumo da banda, em um tráfego com três filas de aplicações distintas, implementadas ora com QoS e LFI e ora sem a QoS e sem a LFI.

5.2.1 - Porquê realizar esses testes.

Estes testes foram realizados tendo como objetivos principais a constatação da execução de intercalação, marcação e classificação dos pacotes, adequação do MGEN e Acterna, os protocolos usados pelos softwares geradores e analisadores de tráfegos, entre outros objetivos.

5.2.2 – Metodologia genérica do cenário de desenvolvimento das medições parciais dos testes de LFI com QoS e análise dos protocolos.

O Enlace Frame Relay [16], [9] do laboratório de teste da OP de 512kbps foi assim distribuído: 52kbps para tráfego *default*; 400 Kbps para FTP; 60kbps para tráfego de tempo real. Foram utilizadas diferentes plataformas – CISCO como Roteadores Cisco - 2600, Cisco - 1751V, Cisco-1760, entre outras que fazem parte do backbone às quais estão conectadas. Conforme representado anteriormente através da Figura-10, foram também utilizados dois *softwares* de geração e análise diferentes: O MGEN e o Examine Acterna e dois Ramais telefônicos. O equipamento *Acterna* captura todo o tráfego gerado a partir do Host02 (ou quaisquer tráfegos que tenham como destino CPE02) na interface de acesso entre o ROT02 e o CPE02 e é analisado pelo software Examine numa máquina Windows conectada ao equipamento Acterna, conforme a ilustração da Figura 10 – representada no capítulo IV, seção - Cenário dos testes e medições. O tráfego passará pelo *backbone* alcançando um dos CPE's 01 ou 03 conforme o teste. Para os testes de telefones usou-se o enlace partindo do CPE02 ao CPE03, onde estavam conectados os ramais telefônicos. O MGEN foi também usado nos testes usando os ramais telefônicos para gerar pacotes grandes que disputavam o meio com pequenos frames de fluxos de voz em tempo real. Assim se previu uma das condições necessárias para implementar e testar a fragmentação com intercalação de pacotes, pois os pacotes grandes de dados precisavam ser fragmentados para não introduzirem grandes valores de jitter aos pequenos pacotes de fluxo de voz e, estes, por sua vez como não devem ser fragmentados são, então, inseridos entre os fragmentos resultantes. Os resultados que se seguem foram extraídos dos softwares – MGEN e Acterna. Sendo assim, são capturados os resultados dos tráfegos gerados e dos respectivos fragmentos, bem como os demais fluxos que concorrem para a mesma banda em disputa. O fato de ocorrer a fragmentação quer dizer que de alguma forma a QoS foi habilitada e, por conseguinte, as políticas de QoS de entrada e saída dos

tráfegos foram devidamente negociadas para que o tráfego de voz tenha êxito e seja viável.

5.2.2.1 - Interpretação I - Dos resultados dessas medições

Na Figura 12 - a seguir é observado a forma como os pacotes são fragmentados e intercalados (LFI com QoS).

Delta time	Size	Destination	Source	Interpretation
10.9 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
15.8 ms	648	DCE	DTE	Frame Relay DLI=100 InformationType=Non D channel user info
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
3.1 ms	194	DCE	DTE	Frame Relay DLI=100 InformationType=Non D channel user info
10.8 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	DTE	Frame Relay DLI=100 InformationType=Non D channel user info
10.7 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	DTE	Frame Relay DLI=100 InformationType=Non D channel user info
12.3 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	DCE	DTE	Frame Relay DLI=100 InformationType=Non D channel user info
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
10.8 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	DTE	Frame Relay DLI=100 InformationType=Non D channel user info
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
10.5 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	DTE	Frame Relay DLI=100 InformationType=Non D channel user info
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
10.6 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	DTE	Frame Relay DLI=100 InformationType=Non D channel user info
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
10.7 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	DTE	Frame Relay DLI=100 InformationType=Non D channel user info
4.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
10.2 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	DTE	Frame Relay DLI=100 InformationType=Non D channel user info
3.5 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
10.2 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	DTE	Frame Relay DLI=100 InformationType=Non D channel user info
3.5 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
10.2 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	DTE	Frame Relay DLI=100 InformationType=Non D channel user info
11.2 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	DCE	DTE	Frame Relay DLI=100 InformationType=Non D channel user info
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
10.7 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	DTE	Frame Relay DLI=100 InformationType=Non D channel user info
10.5 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	DTE	Frame Relay DLI=100 InformationType=Non D channel user info

Figura 12 - Fragmentação com LFI e QoS

O frame (quadro) de voz gerado pelo MGEN teve o tamanho de 194bytes (Len 168 [20 bytes =IP;6 bytes =Frame Relay que totaliza 194bytes) usando o codec G711 tamanho de *payload* é de 160bytes + 8 bytes de UDP totaliza 168bytes de tamanho do datagrama foi intercalado entre os fragmentos UDP de dados. O primeiro fragmento do pacote de dados teve o tamanho de 648bytes de dados cujo tamanho do *payload* FULL foi de 1000bytes ficando 1008 bytes incluindo cabeçalho UDP, logo em seguida é intercalado novamente um frame voz do mesmo tamanho 194bytes, e por conseguinte segue o resto do fragmento de dados FTP (o resto / segundo fragmento) de tamanho de 398bytes incluindo as informações de cabeçalho (20Bytes = IP;8bytes=UDP; 12 bytes = RTP, e 6 bytes = FRF.12). Deste total soma-se 46bytes de *overhead*, por isso se somarmos os 648 bytes de dados adicionado dos 398 bytes do fragmento de dados, teremos um valor superior ao do *payload* inicial de 1000bytes. Estes valores de

cabeçalho foram obtidos a partir das especificações internacionais ITU-T e do CISCO [3],[5].

O tamanho do pacote de dados de *payload* inicial de 1000bytes reproduzidos 50pps foi acrescido de cabeçalhos passando de 1000bytes para um total de 1044bytes (primeiro fragmento de 640bytes payload + 8bytes UDP = 648bytes; segundo fragmento de 360bytes (20Bytes = IP; 8bytes=UDP; 6bytes = FRF.12 + 4bytes de *Frame Check Sequence* (FCS))=398bytes, que são fragmentados em dois fragmentos de 648 bytes e 398 bytes respectivamente para primeiro fragmento e restante fragmento. Com relação aos frames de voz de 194bytes são classificados e marcações como aplicações do tipo tempo real fazendo com que estes jamais sejam fragmentados sobre IP, mas sim intercalados entre os *jumbocargas* – dados grandes de tipo FTP.

Os dados partiram do gerador MGEN origem 10.20.0.2, ou seja, GER02 para o destino 10.10.0.2 (Receptor) REC01. Analisando a Figura-10, verifica-se que as linhas em verde representam os fragmentos resultantes e os da cor castanha representam os pacotes de voz e de dados (o tamanho máximo permitido de pacote que deve passar no link de enlace de 512 Kbps que pelos cálculos padronizados não são mais do que um máximo 640 bytes [20]. Os demais detalhes a nível dos protocolos e políticas de QoS aplicados a cada uma dessas aplicações, referentes aos fluxos de voz e dados da Figura-12 (*Fragmentação com Interleaving LFI e QoS*) - anteriormente citada, estão no Apêndice seção Acterna.

5.2.2.2 - Interpretação II - Dos resultados dessas medições

Conclui-se que todo o tráfego MGEN usa o protocolo UDP, acrescentando-o 8bytes de cabeçalho. Com a LFI habilitada, os valores de jitter para fluxos de voz foram abaixo de 10ms, considerando-se assim um caso ótimo, já que a recomendação aceita 20ms a 30ms.

O *payload* de 1000bytes reproduzidos a uma taxa de 50pps durante 120 000,00 ms, foram fragmentados em dois pedaços, sendo o primeiro de 648 bytes como o tamanho máximo, pois a MTU são de 640bytes para um link de 512kbps. Os pacotes nem sempre foram intercalados na ordem certa, ou seja, houve em alguns casos duas

sequências seguidas de mesmo fluxo. Entretanto, essa não “linearidade” não foi prejudicial para o tráfego de voz.

O tamanho de frame de voz de 194bytes teve frame *checksum – good*, trocados entre a entidades DTE fonte e DCE destino do frame Relay conforme a teoria recomendada.

Para esse teste, mesmo para as classe business o jitter foi em média de 10.8 ms para um datagrama de tamanho (size) 648bytes referente ao primeiro fragmento, endereço de destino 10.10.0.2 e endereço de origem de 10.20.0.2, embora para datagrama o valor de jitter possa ser na ordem de centenas de ms, pois o datagramas de dados não são sensíveis ao atraso, mas sim perda.

Com relação aos parâmetros de QoS para a classe voz, foi setado o *bit* de controle de fragmento setado para 1 (um) que equivale a “*don’t fragment*”, ToS (*Type of Service*) setados para baixo *delay*, alto *throughput*, entre outros aspectos igualmente relevantes detalhado na no Apêndice I – seção Acterna.

5.3 Testes adicionais usando gerador acterna e ramais telefônicos sem QoS/LFI

Nesta seção, pretende-se mostrar os resultados obtidos de forma concreta usando dois telefones, precisamente os ramais 3000 e 5000, sendo que o primeiro conectado no CEP03 e o segundo conectado no CPE02 e o equipamento acterna conectado no CPE02 e no fraccionador, conforme ilustra a Figura 10 - Topologia lógica UFF – OP do Capítulo IV.

O procedimento de teste com os telefones foram:

- 1º - Preparar o MGEN para começar a gerar tráfego. Este aguarda pelo momento adequado;
- 2º - Acionar o Acterna Examine para começar a capturar todos os tráfegos na sua interface;
- 3º - Realizar a ligação telefônica de R3000 ao R5000 começa a chamar então;
- 4º - Acionar o MGEN, começando a gerar um tráfego tipo FTP (a ser fragmentado e intercalado);
- 5º - Devido à configuração nos roteadores dos fluxos de voz, esses pacotes são então intercalados entre os fragmentos ftp;
- 6º - Ao acabar o tempo de execução da geração do tráfego mgen, o acterna deve ser parado;

7º - Finalmente, analisam-se as estatísticas que são semelhantes às referidas a cima em conjunto com a conversação feita via os dois ramais.

Os passos 4º e 5º não foram executados, pois, para este teste inicial, apenas fluxos RTP (voz), foi testado através da conversa entre duas pessoas a fim de avaliar o comportamento da voz sem a compartilha da banda. Foi reservada 60kbps dos 512kbps sem a compressão RTP.

Sendo assim este teste inicial foi sem políticas de QoS e com apenas um tráfego de tempo real contendo um único fluxo de voz oriundo da conversa entre os dois ramais.

Conclui-se, portanto, que teve predominantemente sequências de fluxos RTP, apesar de inicialmente constarem alguns protocolos que se mostraram necessários para sinalizar, estabelecer e negociar conexão. Como já era de se esperar, a viabilidade da comunicação foi ótima, pois, a rede foi dedicada exclusivamente a um tráfego de voz (apesar de ter sido reservado apenas 60kbps, capacidade suficiente para trafegar usando o codec G729 [5]) cujo payload foi de 66bytes a uma taxa de 50pps durante (dois) 2 minutos, usando o codec G729.

Apesar de não haver a compressão de cabeçalho o tráfego comportou-se bem com jitter médio de 16ms e máximo de 19,8ms. Os frames de voz não foram fragmentados porque não tiveram a banda compartilhada com pacotes de dados. Essa situação não costuma acontecer no dia a dia, onde a banda é subutilizada, ou seja dedicada a um tráfego de voz, usando apenas um canal de 60kbps. No dia-a-dia a rede é normalmente ocupada com mais tráfegos, ou seja, além de tráfegos RTP's de voz, teria pelo menos mais dois tipos de tráfegos : videoconferência e dados.

5.4 - Testes Medições com fragmentação usando acterna medição sem QoS e LFI habilitado nas interfaces e usando ramais telefônicos para conversa interativa.

Os 20ms [10] são o intervalo de tempo máximo e constante entre a recepção e a chegada de um frame de voz, não devendo haver variação de atraso que comprometa estes valores, conforme as especificações e as recomendações técnicas.

Em termos práticos: Usando Acterna (Analisador essencialmente de L2) conseguiu-se verificar integralmente a sequência da intercalação dos diversos pacotes, bem como o resto dos seus fragmentos, tal como a teoria recomenda, bem como os parâmetros de QoS e a disposição dos quadros e pacotes em um determinado tráfego quando não ocorre a fragmentação e a inserção dos quadros de tempo real.

A Figura 13 - a seguir, representa o resultado das medidas dos testes sem QoS e sem LFI habilitado usando o G729 e sem cRTP.

DeltaTime	Size	IP	UDP	RTP	Interpretation
81.4 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1945 Timestamp=1644676065 SSRC=0x0F5C0006	
1.1 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1946 Timestamp=1644676225 SSRC=0x0F5C0006	
1.1 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1947 Timestamp=1644676385 SSRC=0x0F5C0006	
1.1 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1948 Timestamp=1644676545 SSRC=0x0F5C0006	
1.1 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1949 Timestamp=1644676705 SSRC=0x0F5C0006	
6.1 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1950 Timestamp=1644676865 SSRC=0x0F5C0006	
20.4 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1951 Timestamp=1644677025 SSRC=0x0F5C0006	
20.2 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1952 Timestamp=1644677185 SSRC=0x0F5C0006	
20.4 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1953 Timestamp=1644677345 SSRC=0x0F5C0006	
20.1 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1954 Timestamp=1644677505 SSRC=0x0F5C0006	
18.8 ms	66	192.168.0.10		192.168.0.6 RTP G.729 Audio Seq=2086 Timestamp=11200 SSRC=0x0F930006	
1.5 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1955 Timestamp=1644677665 SSRC=0x0F5C0006	
14.7 ms	1034	10.30.0.2		10.20.0.2 UDP D=COMPLEX_LINK S=X Windows Len=1008	
2.8 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1956 Timestamp=1644677825 SSRC=0x0F5C0006	
37.0 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1957 Timestamp=1644677985 SSRC=0x0F5C0006	
3.5 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1958 Timestamp=1644678145 SSRC=0x0F5C0006	
20.0 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1959 Timestamp=1644678305 SSRC=0x0F5C0006	
20.0 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1960 Timestamp=1644678465 SSRC=0x0F5C0006	
28.4 ms	66	192.168.0.10		192.168.0.6 RTP G.729 Audio Seq=2087 Timestamp=11360 SSRC=0x0F930006	
16.2 ms	1034	10.30.0.2		10.20.0.2 UDP D=COMPLEX_LINK S=X Windows Len=1008	
1.3 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1961 Timestamp=1644678625 SSRC=0x0F5C0006	
1.1 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1962 Timestamp=1644678785 SSRC=0x0F5C0006	
14.0 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1963 Timestamp=1644678945 SSRC=0x0F5C0006	
23.5 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1964 Timestamp=1644679105 SSRC=0x0F5C0006	
17.0 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1965 Timestamp=1644679265 SSRC=0x0F5C0006	
50.8 ms	66	192.168.0.10		192.168.0.6 RTP G.729 Audio Seq=2088 Timestamp=11520 SSRC=0x0F930006	
16.2 ms	1034	10.30.0.2		10.20.0.2 UDP D=COMPLEX_LINK S=X Windows Len=1008	
1.4 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1966 Timestamp=1644679425 SSRC=0x0F5C0006	
1.1 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1967 Timestamp=1644679585 SSRC=0x0F5C0006	
1.1 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1968 Timestamp=1644679745 SSRC=0x0F5C0006	
7.8 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1969 Timestamp=1644679905 SSRC=0x0F5C0006	
96.5 ms	66	192.168.0.10		192.168.0.6 RTP G.729 Audio Seq=2089 Timestamp=11680 SSRC=0x0F930006	
16.2 ms	1034	10.30.0.2		10.20.0.2 UDP D=COMPLEX_LINK S=X Windows Len=1008	
1.4 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1970 Timestamp=1644680065 SSRC=0x0F5C0006	
1.1 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1971 Timestamp=1644680225 SSRC=0x0F5C0006	
1.1 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1972 Timestamp=1644680385 SSRC=0x0F5C0006	
1.1 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1973 Timestamp=1644680545 SSRC=0x0F5C0006	
3.9 ms	166	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1974 Timestamp=1644680705 SSRC=0x0F5C0006	
1.1 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1975 Timestamp=1644680865 SSRC=0x0F5C0006	
16.2 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1976 Timestamp=1644681025 SSRC=0x0F5C0006	
20.5 ms	66	192.168.0.6		192.168.0.10 RTP G.729 Audio Seq=1977 Timestamp=1644681185 SSRC=0x0F5C0006	

Figura 13 - dos testes sem QoS e sem LFI habilitado usando o G729 e sem cRTP

Na ligação do R3000 ao R5000, ao responder a chamada (R5000), quem escutou no R3000, recebeu simplesmente uma ligação com alto nível de ruído tornando inviável a comunicação. Falando do R5000 ao escutar no R3000 a ligação tornou-se altamente inviável a prática de conversação, pois, apresentava ruídos com cortes de palavras e atrasos constantes. Interpretando de uma forma genérica, a causa disso está associada a não fragmentação dos pacotes de dados. Percebe-se que quadros de voz com tamanho de 66bytes disputaram o enlace com datagramas de 1034bytes. Estes já incluem os

respectivos cabeçalhos. Os 1034bytes são os pacotes de dados que não foram fragmentados. Esses pacotes não fragmentados incluem um atraso grande e a variação desse atraso também será alta, o que prejudicará a aplicação de voz.

Da Figura-13 referenciada anteriormente, ainda na coluna (*size*) percebe-se que todos os pacotes de dados são do mesmo tamanho e foram aparecendo “intercalados” de forma bastante aleatória entre os quadros de voz, conclui-se que esta operação contribuiu para o aumento de atraso de serialização dos quadros RTP na entrada da interface, já que os quadros de voz teriam que esperar um tempo além do recomendado para serem enviados.

Usando os dois ramais telefônicos, dado que havia de cada lado pelo menos uma pessoa escutando e ou falando, era naturalmente perceptível o análise da qualidade do sinal de voz que, conforme dito anteriormente, apresentava altos picos de retardos e cortes na sequência de fala.

Por outro lado, de acordo com o resultado ilustrado (Figura -13), a variação do atraso registrado na coluna (*DeltaTime*) foi na ordem de 81.4ms, 37ms, 28.4ms, 23.5ms, 50.8ms, 95.5ms e vários outros valores acima de 20ms.

Os testes preliminares sem QoS e sem LFI habilitado, segundo a Tabela-8, os valores do jitter são em média elevados. Conclui-se ainda que para todos os tráfegos foram reproduzidos três fluxos concorrentes sendo um fluxo com características de tráfego tempo real (voz) usando o codec G711, um segundo com características de um fluxo *ftp* de 1500bytes e o terceiro um fluxo também de dados colocado na fila da classe *default* com um tamanho de *payload* de 200kbps. Assim, dessas análises concluiu-se que os testes com QoS e LFI habilitado tiveram melhor desempenho nos quesitos banda média ocupada, *jitter* e perda de pacotes. Esses tráfegos receberam cada um os percentuais a seguir indicados, da banda que foram alocados do Enlace *FRF. 12* do laboratório de teste da OP que tem um total de 512kbps:

- 52kbps para trafego *default*;
- 400kbps a sessão FTP;
- 60kbps a tráfego de tempo real (voz).

Esta distribuição da banda deve ser levada em conta a fim de se separar filas distintas e com políticas de QoS próprias que merecem ser respeitadas a fim de garantir a QoS fim-a-fim no enlace ponto-a-ponto, embora neste teste em particular se tenham testado tráfegos sem provisão de QoS.

5.4.1 – Resultado da comparação do desempenho da rede com e sem QoS/LFI - MGEN.

Os resultados da Tabela-8, a seguir representam a relação mediana das perdas e da ocupação da banda; foram feitos baseados nos resultados médios do tráfego incluindo os três fluxos ou invés de cada fluxo, pois, o MGEN, permite gerar tráfegos *Multicasting* em que um único tráfego pode suportar vários fluxos concorrentes para mesmo destino e/ou destino distintos.

	Com QoS e com LFI	Sem QoS e sem LFI
Jitter (Máximo)	15.8ms	81.4ms a 2.722 sec
Perda (%)	0.0% a 6.9%	58%
Banda Consumida (Média %)	75%	+100%
Tempo Médio Teste Telefônico	120sec	10sec
Q ^{tdes} de Fluxos por Tráfego	3	3

Tabela 8 - Fragmentação com e sem LFI e QoS

Ainda dos resultados obtidos, valores de altos picos representam o motivo da degradação da qualidade do sinal da voz, motivado principalmente por não fragmentação do pacote de dados além de outros fatores como congestionamento de enlace. A teoria recomendada segundo os padrões de medidas internacionais e do fabricante que os quadros de voz transmitidos devem chegar a intervalos de tempo constante de no máximo a cada 20ms, ou seja, para aplicações de tempo real como voz, a serialização do atraso recomendado a que os quadros devem passar nas interfaces de saída é de 10ms e não deverá exceder a 20ms. Portanto, não deve haver variações de atrasos que comprometa ainda mais esses valores, pois no caso em estudo, as variações em média superaram o limite antes recomendado. [10], [11].

5.4.1.1 – Interpretação III - Dos resultados dessas medições

Os altos valores de atraso e jitter obtidos nestes testes já eram esperados, na medida em que uma das condições para trafegar e comportar voz sobre redes que

comutam pacote é a realização de LFI. Mesmo tendo banda disponível no enlace para o tráfego de voz e um *ftp*, observou-se que o retardo fim-a-fim, causado pela saída antecipada dos pacotes de 1500bytes, na rede, sem o mecanismo de intercalação foi acima do recomendado, mesmo quando o CIR (*Committed Information Rate*) era garantido, ou seja, a taxa inferior ao limite da garantia negociada.

Concluiu-se que independentemente da taxa de reprodução, banda disponível e que independente do valor de delay (atraso) que os pacotes e ou os quadros toleram de acordo com o enlace a que são testados, jitter acima do recomendado dos 20ms degradou a qualidade de sinal da voz na comunicação usando os dois ramais. Conclui-se ainda que a perda de pacotes ocorreu indiscriminadamente, quando não se teve o cuidado de gerenciar adequadamente a banda. O gerenciamento da banda inclui também não colocar volumes de dados de trafego muito acima da capacidade do canal, como foi o caso representado pelo fluxo 03 da Figura 14 - a seguir.

```
#Um exemplo de nao cumprimento das politicas basicas de QoS
#Excedendo o CIR e o BC

START NOW
PORT 6000
INTERFACE eth0
TTL 10

# time flowid ON addr:port pattern rate size [RSUP ???] [TOS XX]

# Fluxo 1: voz - CODEC G.711
00000 1 ON 10.20.0.2:5000 PERIODIC 20.0 160 #consome em BW(Banda)=25,6kbps
#00000 1 ON 10.20.0.2:5000 PERIODIC 500.0 700

# Fluxo 2: video
00000 2 ON 10.20.0.2:5001 PERIODIC 30.0 1700 #consome em BW=408kbps

# Fluxo 3: dados
00000 3 ON 10.20.0.2:5002 PERIODIC 50.0 5200 #BW=2,08Mbps: Pkts=500:T=10s
#00000 3 ON 10.20.0.2:5000 PERIODIC 20.0 4000

10000 1 OFF
10000 2 OFF
10000 3 OFF
# o caracter "~#" significa comentario para aquela linha

# Example line to set IP header TOS bits to a given value (Linux, FreeBSD & NetBSD)
#00000 1 ON 132.250.95.23:5000 PERIODIC 10.0 128 TOS 24
```

Figura 14 - Script MGEN - Controle e Moldagem de Tráfego em FRF.12.

Desse terceiro fluxo da Figura 14 - anteriormente citada, percebe-se que as políticas de controle e modelagem de trafego não foram respeitadas, implicando em um gerenciamento arbitrário da banda, comprometendo o cumprimento das políticas básicas de QoS. Dessa forma, dado o total da banda da rede 512kbps, sendo 400kbps foi reservado para fluxos de dados, então não se aconselha a colocar um tráfego cuja capacidade exceda em 4 (quatro) vezes mais a capacidade total disponível, a fim de evitar descartes de pacotes e congestionamento da rede.

Assim, com o objetivo de testar o comportamento da rede, e a viabilidade das aplicações, foi-se colocando um *payload* de dados de 5200bytes a 50pps, demandando de 2.10Mbps de banda, no mínimo, tendo provocado instabilidade em todas as aplicações com alto valores do *jitter* e alto percentual de descartes, ou seja, resultou nos seguintes resultados:

- Apenas o terceiro fluxo (# Fluxo 3: Dados) utilizou a banda na ordem de 2,08Mbps;
- Neste caso, o tráfego excedeu em larga escala o limite da CIR, e do BC;
- O nosso link total é de 512 000 bps e o limite de 15% (BC – referindo quanto de rajadas em bits por segundo pode ser enviado em unidade de tempo) dos totais 512kbps do CIR.

Da Figura-14 passa-se a especificar e descrever um dos trechos da linha do *script* de configuração do tráfego a ser gerado a partir do MGEN: o “Fluxo 3 – Dados”: do *script*.

“00000 3 ON 10.20.0.2:5002 PERIODIC 50.0 5200 reproduzido em até 10s

- ✓ 00000 → Instante de tempo de início de geração de pacotes;
- ✓ 3 ou 0003 → ID (Identificação) indica o número de fluxos contidos no tráfego;
- ✓ ON 10.20.0.2:5002 → Endereço para onde o tráfego é gerado e a porta destino;
- ✓ PERIODIC → taxa de reprodução periódica;
- ✓ 50.0 | 5200 → Taxa de pacotes por segundos (pps) | Tamanho de payload bytes.
- ✓ 10000 3 OFF → Tempo de duração (10s) em que o fluxo 3 é reproduzido.

OBS: O caractere “#” significa que tudo seguido dele é um comentário.

Todos os fluxos gerados segundo a Figura 14 - foram originários de um tráfego que parte da porta 6000 de uma placa *ethernet* denominada de interface *eth0* do *host* PC03 (Gerador 03) para o receptor host – PC02 cujo endereço é 10.20.0.2, que recebe pela porta 5000 a 5002 sendo que as duas primeiras portas permitem a recepção dos quadros UDP's ao serem priorizados.

Tomando como exemplo o fluxo de voz diz-se que ele tem os seguintes parâmetros: uma reprodução periódica a taxa de 20pps e um payload de dados de 160 bytes, com um TTL = 10 seg, iniciando a geração de pacotes no instante 00000 ms =

00seg, tendo ainda este fluxo uma identificação ID=1 terminando a geração de pacotes no instante 10sec ou seja 10000ms. Seguindo o entendimento sobre o limite do CIR e do BC excedido em quatro vezes superior ao permitido, conforme representa o Fluxo 3 – Dados, pode-se concluir que por causa desse fluxo, a rede ficou sobreutilizada, com *link* saturada gerando os seguintes resultados.

1. 58 % de perda para pacotes de voz;
2. Delay elevados tanto ao valor mínimo como ao médio e ao máximo para dados e voz;
 - Delay mínimo: 156ms
 - Delay Médio: 963ms
 - Delay Maximo: 2.879sec
3. O jitter de 2,722 segundos, ferindo definitivamente, as normas ITU-T VoIP.

A porcentagem de perda, foi calculado baseado nos resultados extraídos da Figura 15 - a seguir.

```

root@xf-x ~# root root 1036 2007-05-18 20:38 411-ctrl
root@formica ELDT_recv_Traf001_18050718 ~# ./mcalc GFFluxo01D15MqoS_Class
MVALC: Version 3.3a1

FLOW: 0001 SOURCE: 10.10.0.2:6400 DESTINATION: 10.20.0.2:5000
  Num pkts recvd : 83
  Join delay : 72167.688 sec
  Recv pkt rate : 7.684 pkt/sec
  Recv data rate : 9.955 kbps
  Pkts dropped : 116
  Ave. Tx Delay : 0.963 sec
  Max. Tx Delay : 2.879 sec
  Min. Tx Delay : 0.156 sec
  Delay variation : 2.722 sec

MVALC: SUMMARY RESULTS
  Number of active flows : 1 flows
  MVALC: Number of groups joined : 0 groups

MVALC: GROUP JOIN LATENCY STATISTICS
MVALC: Ave. group join latency : 72167.688 sec
MVALC: Min. group join latency : 72167.688 sec
MVALC: Max. group join latency : 72167.688 sec

MVALC: DATA TRANSMISSION LATENCY STATISTICS (Time-sync'd machines required!)
MVALC: Ave. data latency : 0.963 sec
MVALC: Min. data latency : 0.156 sec
MVALC: Max. data latency : 2.879 sec

MVALC: PER-FLOW DATA LATENCY VARIATION
MVALC: Ave. latency variation : 2.722 sec
MVALC: Min. latency variation : 2.722 sec
MVALC: Max. latency variation : 2.722 sec

MVALC: PACKET RECEPTION STATISTICS
MVALC: Total packets received : 83 pkts
MVALC: Total recv packet rate : 7.684 pkt/sec
MVALC: Total recv data rate : 9.955 kbps
MVALC: Est. num pkts dropped : 116 pkts
root@formica ELDT_recv_Traf001_18050718 ~#
  
```

Figura 15 - Resultado a partir do MGEN para testes sem QoS
 no fato e que dos 200 pacotes transmitidos do fluxo de voz (20pps * 10s), 116 foram descartados e apenas foram recebidos 84 pacotes sendo que os demais fluxos sequer entraram na interface.

5.4.1.2 - Interpretação IV - Dos resultados dessas medições

Concluiu-se que: a LFI, depende da aplicação QoS independentemente das suas políticas de entrada e ou saída das interfaces dos roteadores. Percebeu-se também que o descumprimento de um dos parâmetros do FRTS – CIR (Taxa média de dados por unidade de tempo) degrada a qualidade do sinal; que ao introduzir valores muito acima

do CIR provocou instabilidade na rede. Notou-se ainda que ao introduzir valor de taxa de *pps* bem como o tamanho de *payload* de *pps* indevidamente mensurados, com relação a QoS fim a fim conforme configurado nas plataformas e negociado entre as partes, causando também perda e altos valores de *delay* e suas variações, além de comprometer a estabilidade de toda a rede, elevar o nível de processamento, tornando inviável em média 89% de todas as aplicações, como os dos testes de voz²⁰, dados conforme a Figura a seguir.

A Figura 15, anteriormente, referenciada é uma das ilustrações considerada como exemplo para base de cálculo dos resultados estatísticos que somado aos demais resultados obtidos, apurou-se a média da inviabilidade das aplicações para os respectivos testes equivalentes.

5.5 - TESTES DE FRAGMENTAÇÃO USANDO ACTERNA MEDIÇÃO COM QoS E LFI.

Nestes testes uma vez levando em consideração as políticas de QoS e LFI habilitada, preservou-se a integridade dos pacotes marcados como prioritários independentes do tamanho dos demais fluxos, quando de fato estes receberam a tal marcação. Mesmo com a QoS e LFI, o congestionamento do *link* inviabilizou as aplicações independentemente das suas classificações, quando assim foram realizados testes com tais propósitos.

Quando um fluxo de voz devidamente marcado e classificado, atendendo critérios de QoS como *delay* baixo, precedência ECP (*Encryption Control Protocol*) crítica e alta vazão, etc, resultaram que os pacotes chegaram às suas interfaces de saída em intervalo de tempo constante menor que os 20ms recomendados pelas normas de padronização internacionais.

Já nos testes com aplicação de LFI e pacotes gerados pelo MGEN conforme mostrado na Tabela 8, onde foram comparados os resultados dos parâmetros implementados, os valores notados foram abaixo de 20ms em media 15.8ms. O fato de

²⁰ Uma aplicação VoIP torna-se impraticável na presença de grandes e constantes atrasos e as suas variações; parâmetros dos quais uma aplicação do tipo voz sob-demanda é muito sensível, neste caso estas técnicas e LFI impõem solução a rede a esta aplicação sem ter que separar a rede de telefonia a rede de dados e multimídia.

ter ocorrido a LFI conforme a Figura -16, a seguir, deu para perceber ainda que os quadros foram intercalados ao rigor das boas práticas aconselhadas.

DeltaTime	Size	Destination	Source	Interpretation
10.9 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
15.8 ms	648	10.10.0.2	10.20.0.2	Frame Relay DLCI=100 InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
3.1 ms	194	10.10.0.2	10.20.0.2	Frame Relay DLCI=100 InformationType=Non D channel user info
10.8 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	10.20.0.2	Frame Relay DLCI=100 InformationType=Non D channel user info
10.7 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	10.20.0.2	Frame Relay DLCI=100 InformationType=Non D channel user info
12.3 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	DCE	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
3.1 ms	194	10.10.0.2	10.20.0.2	Frame Relay DLCI=100 InformationType=Non D channel user info
10.8 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	DCE	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
10.5 ms	648	10.10.0.2	10.20.0.2	Frame Relay DLCI=100 InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
10.6 ms	648	10.10.0.2	10.20.0.2	Frame Relay DLCI=100 InformationType=Non D channel user info
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	DCE	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
10.6 ms	648	10.10.0.2	10.20.0.2	Frame Relay DLCI=100 InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
10.7 ms	648	10.10.0.2	10.20.0.2	Frame Relay DLCI=100 InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
4.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
10.2 ms	648	10.10.0.2	10.20.0.2	Frame Relay DLCI=100 InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
3.5 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
10.2 ms	648	10.10.0.2	10.20.0.2	Frame Relay DLCI=100 InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
3.5 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
10.2 ms	648	10.10.0.2	10.20.0.2	Frame Relay DLCI=100 InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
11.2 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	10.20.0.2	Frame Relay DLCI=100 InformationType=Non D channel user info
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
10.7 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
3.1 ms	194	10.10.0.2	10.20.0.2	Frame Relay DLCI=100 InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
10.5 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
3.1 ms	194	10.10.0.2	10.20.0.2	Frame Relay DLCI=100 InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168

Figura 16 - Aplicação de LFI a rede de pacotes com frame de voz simulado pelo MGEN

Percebe-se ainda que se obteve dois tipos de quadros, o do tipo UDP, referindo aos pacotes de dados gerados pelo MGEN e o do tipo Frame Relay DLCI 100. Foram reproduzidos, portanto, dos fluxos ftp 50pps dos 1000bytes transmitidos ao serem fragmentados geraram-se dois fluxos para cada 1pps sendo um tipo UDP e o outro Frame Relay DLCI = 1000, ou seja, para cada um pacote por segundo de 1000bytes gerou-se dois fluxos: por exemplo um de UDP 648bytes e ou outro fluxo Frame Relay DLCI de 398bytes que correspondem aos fragmentos restantes do tráfego UDP original. Esses dois fluxos referidos já incluem o valor de *overhead* assim, um terceiro fluxo prioritário de tamanho 160bytes também se faz presente nesta Figura-16 dado que estes pacotes pequenos como não devem ser fragmentados foram então intercalados entre os fluxos *ftp* e os respectivos fragmentos gerados.

Os tráfegos com baixos valores e ou nos limites dos parâmetros de FRTS fluíram normalmente. Sem QoS pacotes sofreram perda indiscriminadamente, principalmente se os parâmetros para modelagem *Frame Relay Traffic Shaping* - FRTS não forem respeitados, ou seja, valores acima dos parâmetros como por exemplo CIR, negociados

pela modelagem FRTS, pois a tecnologia de protocolo de enlace foi baseada em Frame Relay.

A fim de prover QoS (DiffServ), criou-se algumas classes de serviço, nomeadamente, Classe Business, Classe Voz além da classe default, conforme a Tabela-6, anteriormente referenciada. Essas diferentes classes receberam classificações também diferentes a fim de prover prioridades a determinados fluxos as marcações foram EF e AF31 para as classes voz e business respectivamente o que quer dizer respectivamente prioridade alta e intermediária. Com habilitação de Intercalação, os frames de voz - fluxos RTP, classe voz, marcação – EF, sempre receberam preferência na alocação de banda entre os demais frames da classe Business - marcação AF31, baixando o *jitter* de aplicação de tempo real da ordem 2,722sec a 22ms para em média 14ms ou valores menores.

Os frames capturados nos testes de tráfego de tempo real usando os dois ramais, não foi usado o gerador MGEN, mas sim conversas usando dois ramais telefônicos e o Acterna conforme representa a ilustração - Figura 17 a seguir. Conforme dito anteriormente, foram extraídos levando em conta a aplicação de QoS ponto-a-ponto, e por conseguinte habilitada a fragmentação e intercalação (LFI) de pacotes.

DeltaTime	Size	Destination	Source	Interpretation
5.6 ms	66	192.168.0.6	192.168.0.10	RTP G 729 Audio Seq=370 Timestamp=1549523941 SSRC=0x0DD9000A
8.1 ms	648	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	DTE	Frame Relay DCE=100 InformationType=Non D channel user info
5.6 ms	66	192.168.0.6	192.168.0.10	RTP G 729 Audio Seq=371 Timestamp=1549524101 SSRC=0x0DD9000A
8.1 ms	648	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
5.9 ms	66	192.168.0.6	192.168.0.10	RTP G 729 Audio Seq=372 Timestamp=1549524261 SSRC=0x0DD9000A
11.0 ms	648	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	DTE	Frame Relay DCE=100 InformationType=Non D channel user info
220 us	66	192.168.0.6	192.168.0.10	RTP G 729 Audio Seq=373 Timestamp=1549524421 SSRC=0x0DD9000A
16.2 ms	648	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
3.9 ms	66	192.168.0.6	192.168.0.10	RTP G 729 Audio Seq=374 Timestamp=1549524581 SSRC=0x0DD9000A
2.4 ms	398	DCE	DTE	Frame Relay DCE=100 InformationType=Non D channel user info
13.7 ms	648	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
4.4 ms	66	192.168.0.6	192.168.0.10	RTP G 729 Audio Seq=375 Timestamp=1549524741 SSRC=0x0DD9000A
1.9 ms	398	DCE	DTE	Frame Relay DCE=100 InformationType=Non D channel user info
13.7 ms	648	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
4.4 ms	66	192.168.0.6	192.168.0.10	RTP G 729 Audio Seq=376 Timestamp=1549524901 SSRC=0x0DD9000A
1.9 ms	398	DCE	DTE	Frame Relay DCE=100 InformationType=Non D channel user info
13.7 ms	648	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
4.9 ms	66	192.168.0.6	192.168.0.10	RTP G 729 Audio Seq=377 Timestamp=1549525061 SSRC=0x0DD9000A
1.4 ms	398	DCE	DTE	Frame Relay DCE=100 InformationType=Non D channel user info
13.9 ms	648	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
4.7 ms	66	192.168.0.6	192.168.0.10	RTP G 729 Audio Seq=378 Timestamp=1549525221 SSRC=0x0DD9000A
1.6 ms	398	DCE	DTE	Frame Relay DCE=100 InformationType=Non D channel user info
9.9 ms	157	192.168.0.6	192.168.0.10	R 225.0 CONNECT IEI=Bearer Capability Location=User User_Msg
3.6 ms	648	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
5.4 ms	66	192.168.0.6	192.168.0.10	RTP G 729 Audio Seq=379 Timestamp=1549525381 SSRC=0x0DD9000A
900 us	398	DCE	DTE	Frame Relay DCE=100 InformationType=Non D channel user info
13.8 ms	648	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
5.5 ms	66	192.168.0.6	192.168.0.10	RTP G 729 Audio Seq=380 Timestamp=1549525541 SSRC=0x0DD9000A
800 us	398	DCE	DTE	Frame Relay DCE=100 InformationType=Non D channel user info
1.1 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=381 Timestamp=1549525701 SSRC=0x0DD9000A
12.6 ms	648	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.0 ms	66	192.168.0.6	192.168.0.10	RTP G 729 Audio Seq=382 Timestamp=1549525861 SSRC=0x0DD9000A
290 us	398	DCE	DTE	Frame Relay DCE=100 InformationType=Non D channel user info
1.1 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=383 Timestamp=1549526021 SSRC=0x0DD9000A
10.2 ms	648	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	DCE	DTE	Frame Relay DCE=100 InformationType=Non D channel user info
1.1 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=384 Timestamp=1549526181 SSRC=0x0DD9000A
1.5 ms	66	192.168.0.6	192.168.0.10	RTP G 729 Audio Seq=385 Timestamp=1549526341 SSRC=0x0DD9000A
14.1 ms	648	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
5.9 ms	66	192.168.0.6	192.168.0.10	RTP G 729 Audio Seq=386 Timestamp=1549526501 SSRC=0x0DD9000A

Figura 17 - Aplicação de LFI e QoS a redes de pacotes priorizando os quadros de voz.

A habilitação de intercalação permitiu que os valores de jitter sejam abaixo do limite máximo recomendado o que garante afirmar que a aplicação de tempo real foi ótima ao longo da conversação telefônica, verificou-se uma intercalação dos pacotes exatamente como o padrão recomenda. Além do fluxo *ftp* que teve como protocolo de transporte o UDP e o seu respectivo fragmento Frame Relay DLCI, é apresentado outro fluxo - fluxo RTP que representa realmente os quadros de voz intercalados entre o UDP e o Frame Relay DLCI.

5.5.1 – Interpretação V - Dos resultados dessas medições

A LFI aplicado QoS em uma situação de muito estresse na rede, evitou altos *delay*, *jitter* e perdas de informações, passando das mesmas circunstâncias de utilização de enlace, de uma percentagem de 58% de perda para 6,9%. de informação em todo o enlace.

Vale ainda destacar que os testes de LFI foram realizados sem compressão RTP e com compressão RTP e os resultados das aplicações são de um modo geral bons conforme se pode perceber nos testes complementares da LFI que seguem mais adiante. Com isso pode-se dizer que os mecanismos de QoS como estes, permitem que uma rede de dados comporte tráfego de voz, pois mesmo em casos onde havia banda sobrando na ordem de 40%, ficando portanto impraticável a comunicação na presença de altos valores de descartes de pacotes e jitter elevados conforme pode ser verificado na Figura 46Figura-17.

A sequência²¹ da intercalação dos pacotes (voz e dados) fluxos-a-fluxos foram na ordem seguinte:

RTP – Fluxo de voz em tempo real cujo tamanho é de 66bytes, seguido de fluxo;
 UDP – Fluxo ftp de tamanho 648 bytes, primeira sequência de total dos 1008 bytes;
 RTP – Fluxo de voz em tempo real cujo tamanho é de 66bytes, seguido de fluxo;

21

Note que a sequência dos fluxos não é necessariamente linear, o que não compromete a eficácia do experimento em teste não afetando, portanto, a viabilidade da aplicação, concluímos, portanto que a ordem de intercalação não precisa ser necessariamente linear, ou seja, na ordem, RTP –UDP- RPT – Fragmento Frame Relay.

Frame Relay – Fragmento do fluxo ftp restante dos iniciais 1008 bytes;
 UDP – Fluxo ftp de tamanho 648 bytes, primeira sequência de total dos 1008 bytes;
 RTP – Fluxo de voz em tempo real cujo tamanho é de 66bytes, seguido de fluxo;
 Frame Relay – Fragmento do fluxo ftp restante dos iniciais 1008 bytes;

OBS:

- ✓ UDP – Protocolo nato, usado pelo gerador MGEN para gerar os dados de 1000bytes;
- ✓ Frame Relay – Protocolo de nível dois associado aos fluxos fragmentados;
- ✓ RTP – Protocolo de nível de aplicação usado para os serviços de tempo real.
- ✓ O FTP referido neste trabalho não se refere ao tipo de protocolo, mas sim ao tipo de dados de sistema de arquivos podendo ser em formato de imagem (conjunto contínuo de bits), dados locais (bytes lógicos) [19], etc.

Esta sequência podia estar representada de forma inversa assim como tendo duas sequências de RTP e ou UDP e Frame Relay seguidas. Conclui-se ainda, que os resultados foram indiscutivelmente, ótimos. O quesito jitter foi bastante bom se comparado com os tráfegos que não foram implementadas políticas de QoS. Apenas para os fluxos ftp 50pps dos 1000bytes a serem fragmentados, são gerados dois fluxos para cada 1pps sendo um tipo UDP e o outro Frame Relay DLCI = 100, ou seja, para cada 1 (um) pacote por segundo de 1000bytes serão gerados dois fluxos: um de UDP 648bytes e ou outro fluxo Frame Relay DLCI de 398bytes que corresponde ao fragmento restante do tráfego UDP original. Se, portanto, forem gerados 50pps de fluxo *ftp* em 2min = 120sec, quer dizer que seriam gerados 6000 pacotes de tamanho 1000bytes de payload, o que duplicará ao ser fragmentado, portanto é de certo modo inconveniente capturar os dozes mil (12 000) pacotes que trafegam na rede, por isso capturamos como amostra alguns fluxos.

Esse valor - 12000 refere-se apenas ao tráfego dos fluxos *ftp*, sem levar em conta o tráfego dos fluxos RTP referente à aplicação de tempo real (voz). Com relação às políticas e mecanismos de QoS estão em parte destacados na Tabela-6, onde trecho de configuração de um dos CPEs é mostrado. Pode-se notar algumas classes e marcações explícitas na referida tabela descritas em trechos de *script* da configuração dos roteadores, para as referidas classes de serviços. Ficam ainda claras as políticas de

Controle e Moldagem de Tráfego em Redes *Frame Relay* configuradas e usadas nos teste de LFI, sendo, portanto, implementado e analisador de uma forma geral os serviços *DiffServ*, pois os pacotes foram classificados e marcados de acordo com o tráfego para determinados pacotes a partir de uma dada classe de serviço (CoS) . Em face disso a linha de arquitetura para provisão de QoS foi *DiffServ*. Sendo assim, uma das formas utilizadas para implementar CoS (*Class Of Service*), foi atribuindo prioridades às classes baseadas na precedência comportamental dos pacotes e ou quadros que receberam marcações separadas e distintas.

Durante todos os testes realizados, conforme consta do resumo - *abstract* desta Dissertação, foi levado sempre em conta a questão de QoS. A QoS, embora, esteja intimamente associada às redes orientadas a conexão teve-se sempre esta preocupação uma vez que a nossa rede é IP/MPLS e com tecnologia de protocolo nível dois - Frame Relay, usando o padrão FRF.12. Como as redes IP não são orientadas a conexão, para simular o estabelecimento de conexão, para que recursos sejam reservados, com objetivo de conferir tratamento adequado aos pacotes que fluem nessas mesmas redes, cria-se “*pseudo – conexões*” através de rotas de circuitos virtuais como rotas MPLS ou de alguma outra forma de priorização do tráfego.

Para as tecnologias de rede nível dois, como Frame Relay recomendação FRF.12, em termos de QoS, teve-se sempre o cuidado de negociar e manter o nível dos parâmetros de QoS como taxas sustentadas e tamanho de rajadas, permitindo a rede alocar recursos para satisfazer determinado perfil de tráfego, mantendo as aplicações dos usuários finais, parâmetros de QoS satisfatórios como níveis baixos de atrasos e pouca perda de pacotes, assim como baixos valores de *jitter*, pois a obediência a políticas negociadas como estas, mesmo em caso de violação de outros parâmetros de QoS durante fases de congestionamento, a rede manteve aceitáveis níveis de qualidade de viabilização das aplicações em termos de valores médios de *jitter*.

5.6 - QUANTO AOS TESTES DE COMPRESSAO DE CABEÇALHO RTP.

Com esses testes, pretende-se medir o consumo da banda, viabilidade das aplicações VoIP, análise dos protocolos que envolvem essas aplicações, inclusive no domínio do backbone, bem como a quantidade de cabeçalho que cada protocolo da

camada de rede coloca as aplicações de voz conforme os pacotes passam nas suas respectivas camadas de rede.

5.6.1 - Porquê realizar esse teste

O objetivo principal dessas medições é avaliar as aplicações VoIP quando estas sofrem compressão RTP e quando estas não sofrem compressão, e também avaliar o consumo da banda com ou sem a cRTP.

5.6.2 - Metodologias das medições dos testes de compressão de cabeçalho RTP.

Para os testes de compressão de cabeçalho foi usado o analisador *Acterna*; foi, entretanto, configurado o CODEC para G.729 com a taxa de transmissão de 8kbps podendo alcançar a taxa máxima de 30kbps com o VAD (*Voice Activity Detector*) desabilitado. A opção de desabilitar o VAD faz com que o roteador gere pacotes por unidade de tempo de forma constante, por exemplo, a 50pps independentemente de ter conversação telefônica ou não evitando que mais recursos sejam desperdiçados. Configurando os ramais: 3000 e 4000 para o CPE02 e Ramais 5000 e 6000 para o CPE03 passando pelo Backbone), assim como alguns parâmetros QoS para classificação e marcação dos pacotes, bem como habilitar ou não a Compressão de cabeçalho priorizando os tráfegos de tempo real.

A partir das chamadas estabelecidas, verificou-se as estatísticas da quantidade de pacotes gerada e, corretamente comprimidos através do comando *show frame-relay IP RTP headercompression* nos CPE's 02 e 03(origem e destino das chamadas respectivamente) e ou *show police-map interface serial 0/0.1*, já que o roteador CISCO mostra a média dos últimos 30 segundos das estatísticas. Num segundo momento, no mesmo cenário, colocou-se dois fluxos de VOZ em paralelo e repetiu-se os testes com e sem compressão.

5.6.3 - Resumo dos resultados de teste sem compressão.

Observa-se o tamanho do pacote FR com 66 bytes, conforme a Figura-18 a seguir. Mais detalhes sobre esta Figura, encontra-se no Apêndice Seção Compressão de Cabeçalho RTP.

Number	DeltaTime	Size	Destination	Source	Interpretation
1	960 us	16	DTE	DTE	DTE T1 617 Annex D STATUS ENQUIRY IE Ident
2	1.2 sec	50	192.168.0.6	192.168.0.10	TCP D=H 225 S=15930 SYN Seq=106426024
3	5.0 ms	50	192.168.0.10	192.168.0.6	TCP D=H 225 S=15930 SYN Seq=106426024
4	2.0 ms	46	192.168.0.6	192.168.0.10	TCP D=H 225 S=15930 Ack=1508282598 Se
5	9.7 ms	351	192.168.0.6	192.168.0.10	H 225 0 Frame Fragmented SETUP IEI=Bea
6	39.5 ms	169	192.168.0.10	192.168.0.6	H 225 0 CALL PROCEEDING IEI=User-User U
7	14.4 ms	134	192.168.0.10	192.168.0.6	H 225 0 PROGRESS IEI=Facility Location=
8	25.8 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=679 Timestamp=0 SSR
9	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=680 Timestamp=160 S
10	20.3 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=681 Timestamp=320 S
11	20.1 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=682 Timestamp=480 S
12	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=683 Timestamp=640 S
13	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=684 Timestamp=800 S
14	17.7 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=685 Timestamp=960 S
15	20.3 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=686 Timestamp=1120 S
16	20.1 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=687 Timestamp=1280 S
17	260 us	46	192.168.0.6	192.168.0.10	TCP D=H 225 S=15930 Ack=1508282609 Se
18	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=688 Timestamp=1440 S
19	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=689 Timestamp=1600 S
20	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=690 Timestamp=1760 S
21	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=691 Timestamp=1920 S
22	20.1 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=692 Timestamp=2080 S
23	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=693 Timestamp=2240 S
24	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=694 Timestamp=2400 S
25	20.1 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=695 Timestamp=2560 S
26	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=696 Timestamp=2720 S
27	20.1 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=697 Timestamp=2880 S
28	17.7 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=698 Timestamp=3040 S
29	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=699 Timestamp=3200 S
30	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=700 Timestamp=3360 S
31	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=701 Timestamp=3520 S
32	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=702 Timestamp=3680 S
33	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=703 Timestamp=3840 S
34	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=704 Timestamp=4000 S
35	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G 729 Audio Seq=705 Timestamp=4160 S

Figura 18 - Pacotes sem compressão capturados no acesso FR de 512K

O examinador Acterna, provou que foi acrescido de: 4bytes de header, além de identificar o campo endereço, o tamanho do frame mais *payload*²² composto pelos *headers*²³ IP/UDP/RTP+dados+*checksum* somando 62 bytes. Da mesma forma, observou-se:

Do pacote IP (payload) 20bytes de cabeçalho, o tamanho total do pacote 60 bytes mais *payload* composto pelos *headers* UDP/RTP+dados+*checksum* somando 42 bytes + 4bytes acrescido pela rede completa os 66bytes. Este tamanho de 66bytes é o valor de payload de quadro de voz sem compressão usando o codec G729; Do datagrama UDP 8bytes de header; nele identificou-se à porta origem e destino, *checksum* que nesse caso não é utilizado. Como os testes foram realizados sem a compressão de cabeçalho percebe-se na terceira coluna que se teve um total de 66bytes para os fluxos RTP, por causa disso, concluiu-se que no primeiro teste realizou-se uma chamada de oito (8) minutos com compressão desabilitada ocupou-se 26Kbps de banda dos 512Kbps de acesso conforme a Tabela 37 - Medição de Compressão com cRTP

²² Payload - Conteúdo de informação útil em um protocolo sem informações de cabeçalho

²³ Headers – cabeçalhos de protocolos de Comunicação.

desabilitado– (Vide Apêndice I Seção Compressão Cabeçalho RTP). Retirando os *headers* dos protocolos FR, IP e UDP, resta apenas o quadro RTP que transporta em seu header o tipo de CODEC, número de sequência, *timestamp*, *SSRC* que somados chegam aos 12 bytes de header mais o payload de 20 bytes referentes à conversação mais 2 bytes de checksum. Em resumo, 66bytes do pacote FULL²⁴ 46bytes são de *header* implicando em 69% de *overhead*, já com a compressão dos 28 bytes do pacote comprimido apenas 4 bytes (2 do CID e 2 do checksum) são de *overhead* o que representou apenas 14% da informação.

5.7 – Resumo do resultado dos testes, mas habilitando a compressão.

Habilitou-se a compressão, ocupou-se 10kbps de banda dos 512kbps conforme Tabela 38 - Medição de compressão com cRTP habilitado. (vide Apêndice I – Seção Compressão de Cabeçalho). Podia-se assim colocar quase 2 fluxos de VOZ a mais em paralelo na banda otimizada para alcançar o valor de apenas um fluxo sem compressão. Conforme dito na teoria sobre compressão de cabeçalho, o primeiro pacote não sofre compressão, somente a partir do segundo quando os roteadores criam o CID (*Context ID*) para aquele fluxo.

5.7.1 - Matriz relacionando parâmetros da rede com modelagem com/sem cRTP

Dos resultados conclusivos afirma-se que segundo a Tabela 9 ocupou-se 5,1% de banda consumida na rede e com compressão o percentual cai para 1,95% de ocupação para apenas 1 fluxo de voz, ou seja, o cabeçalho realmente foi comprimido e tivemos 38,5% de banda economizada.

	Banda Ocupada Kbps %	Qtde Fluxos	Bytes FULL	Qtde Cabeçalho Overhead %	Economia de Banda	Tempo de Experimento
Com Compressão Cabeçalho	10Kbps 1,95%	1	28 bytes	4Bytes 14%	38.5%	8 min
Sem Compressão Cabeçalho	26Kbps 5.1%	1	66 bytes	46bytes 69%	Indisponí vel	8 min

Tabela 9 - Compressão de Cabeçalho e não compressão de cabeçalho

²⁴ FULL: Neste contexto representa um datagrama com os respectivos *overheads*.

Dos resultados analisados com compressão observou-se segundo a Figura 19 - a seguir, que o tamanho do quadro FR com 28bytes, é distribuído da seguinte forma: Dos 28bytes do quadro FR temos 4bytes de header e os 24bytes restante de payload onde contém os 4 bytes do cabeçalho RTP comprimido mais os 20bytes de dados.

Number	DeltaTime	Size	Destination	Source	Interpretation
1		16			DTE T1 617 Annex D STATUS ENQUIRY IE Identifi
2	960 us	16			DCE T1 617 Annex D STATUS IE Identifier=Repor
3	3.0 sec	330			DCE CDP Name=CPE-02 IP Address=192.168.0.6 Pl
4	2.4 sec	50	192.168.0.10	192.168.0.6	TCP D=H 225.0 S=41760 SYN Seq=1026946729
5	3.8 ms	50	192.168.0.6	192.168.0.10	TCP D=41760 S=H 225.0 SYN Ack=1026946730
6	2.4 ms	46	192.168.0.10	192.168.0.6	TCP D=H 225.0 S=41760 Ack=293904192 Seq=1
7	10.5 ms	351	192.168.0.10	192.168.0.6	H 225.0 Frame Fragmented SETUP IEI=Bearer
8	33.1 ms	169	192.168.0.6	192.168.0.10	H 225.0 CALL PROCEEDING IEI=User-User Use
9	5.1 ms	134	192.168.0.6	192.168.0.10	H 225.0 PROGRESS IEI=Facility Location=Us
10	18.9 ms	66			DTE Frame Relay DLCI=100 InformationType=Non
11	19.5 ms	31			DTE Frame Relay DLCI=100 InformationType=Non
12	20.1 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
13	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
14	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
15	20.3 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
16	20.1 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
17	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
18	17.7 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
19	17.1 ms	46			DTE Frame Relay DLCI=100 InformationType=Non
20	3.2 ms	28	192.168.0.10	192.168.0.6	TCP D=H 225.0 S=41760 Ack=293904192 Seq=1
21	20.1 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
22	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
23	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
24	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
25	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
26	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
27	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
28	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
29	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
30	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
31	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
32	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
33	17.6 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
34	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
35	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
36	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
37	20.1 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
38	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non
39	20.2 ms	28			DTE Frame Relay DLCI=100 InformationType=Non

Figura 19 - Pacotes Comprimidos capturados no acesso FR de 512K

O frame passou-se de 66bytes para 28bytes, com ótimo desempenho no quesito consumo de banda que também caiu muito de 100% para 39.07%, a outra diferença, é ao invés de protocolo ser RTP, utilizou-se o Frame Relay DLCI 100 uma vez que a habilitação da compressão de cabeçalho é um parâmetro configurado no acesso Frame Relay ponto-a-ponto quando habilitado a implementação de QoS. O DCE e o DTE são os canais de comunicação frame relay setados para habilitar o frame relay ponto-a-ponto.

5.7.2 – Interpretação dos Resultados parciais da compressão de cabeçalho RTP

Em resumo os 66bytes do pacote FULL 46 bytes são de header implicando em 69% de *overhead*, já com a compressão dos 28 bytes do pacote comprimido apenas 4bytes (2 do CID e 2 do *checksum*) são de *overhead* o que representa apenas 14% da informação.

Conclui-se que dos testes de compressão de cabeçalho, consumiu-se mais de 5.1% do link para um único fluxo de voz, para o mesmo experimento utilizando a

compressão não se utilizou 1.95% do link, num segundo momento com testes realizados utilizando dois fluxos em paralelo sem compressão utilizou-se 10% da banda útil da rede quando se poderia colocar mais de cinco fluxos de voz comprimidos em paralelo ou qualquer outro tipo de aplicação como vídeo, áudio ou dados, a banda que seria consumida por *overhead* utilizara-se para informação útil otimizando o acesso em até 62%. Estes valores de overhead acrescidos ou comprimidos são para dos protocolos: FRF.12/IP/UDP/RTP, além de outros analisados nos testes com os pacotes capturados no backbone IP/MPLS que foram analisados os cabeçalhos dos protocolos como Ethernet (14 bytes de header), MPLS (4 bytes de header) IP, UDP,RTP apresentados no Apêndice I seção Analise em Backbone).

5.8 – Compressão com telas dos pacotes capturados no backbone IP/MPLS

No backbone os pacotes não sofrem compressão, somente no acesso FR do CPE para o *router* de borda da rede IP/MPLS, por esse motivo os pacotes não se mostraram diferentes, foram praticamente iguais em todos os testes, conforme segue.

5.9 - Resultados de testes pré-liminares sobre as medições de CODECs, LFI, cRTP, comportamento da rede, e ocupação da banda por aplicações.

Ao fim desta primeira etapa, concluiu-se que os resultados foram satisfatórios, conforme tem sido relatado ao longo desta dissertação, pois em redes de comunicações, onde além de tráfego de dados comuns, são trafegadas aplicações de tipo multimídia, é altamente recomendável a análise dos itens referenciados inicialmente, pelo que acreditamos ser útil para a provisão e garantia de boas aplicações juntos aos usuários finais.

Seguindo as recomendações das normas dos órgãos de padronização internacionais, apurou-se, efetivamente, que os resultados são comprovados de acordo com as mesmas recomendações, se seguidas e respeitadas as metodologias recomendadas pelos padrões internacionais e de acordo com as especificações dos fabricantes. Ademais, durante os testes, pode-se comprovar nitidamente e de forma real a viabilidade ou a não viabilidade das aplicações durante a realização de alguns testes dos quais, por exemplo, usávamos os ramais telefônicos para conversar, escutar e analisar o grau de inteligibilidade das conversações.

5.9.1 Quantos aos CODECs testados:

Quanto aos testes dos codecs realizados, conclui-se mais precisamente que:

- Com equipamento CISCO e o CODEC G.726, conseguiu-se o segundo melhor resultado com uma tolerância de 42,0% perdendo apenas para o equipamento HP-3800 usando o CODEC G.711 – 43,5%, apesar do CISCO ter apresentado em média melhor resultado com relação aos demais equipamentos, usando os quatro CODEC's que foram analisados.
- Percebeu-se também que os CODECs G711 e G726 são mais tolerantes a perda de pacotes. O CODEC G729 vem em seguida com boa tolerância a perda. Por último, o G723 é o menos tolerante a perda de pacotes. Observou-se, também, que o roteador Cisco e o PABX Siemens apresentam maiores valores para tolerância a perda de pacotes.

5.9.2 - Quanto aos testes de compressão:

Perante os testes realizados sobre a compressão de cabeçalho concluiu-se que:

- Quando os experimentos foram realizados sem compressão ocupou-se 5,1% de banda consumida na rede e com compressão a percentagem cai para 1,95% de ocupação para apenas 1 fluxo de voz tanto para teste com cabeçalho comprimido e também para testes sem cabeçalho comprimido durante longos oito minutos, o que leva a conclusão de que com o cabeçalho comprimido conseguiu-se 38,5% de banda economizada, pois os pacotes não comprimidos os cabeçalhos tem um tamanho nominal de 66bytes e quando comprimido reduzem-se para 28bytes, somando simplesmente 14% de overhead se comparado com os mesmos testes em que não foi comprimido o cabeçalho resultando em 69% de *overhead*.
- Percebeu-se ainda que nos testes de compressão de cabeçalho, consumiu-se mais de 5.1% do link para um único fluxo de voz, para o mesmo experimento utilizando a compressão não se utilizou 1.95% do link, num segundo momento com testes realizados utilizando dois fluxos em paralelo sem compressão utilizou-se 10% da banda útil da rede quando poderia se colocar mais de cinco

fluxos de voz comprimidos em paralelo ou qualquer outro tipo de aplicação como vídeo, áudio ou dados, a banda que seria consumida por overhead utilizasse-se para informação útil otimizando o acesso em até 62%.

5.9.3 - Quanto aos testes de fragmentação com intercalação:

Com relação aos testes de fragmentação e intercalação de pacotes, apurou-se, em resumo, o seguinte:

- que, conforme se pode ler na Tabela 8 - a Fragmentação com e sem LFI e QoS, apresentou particulares vantagens do uso da técnica de intercalação de pacotes na medida em que para as mesmas quantidades de fluxos por tráfego - três fluxos (vide Tabela 8), e apesar de uma alta discrepância do tempo de processamento da simulação dos testes - 120seg * 10seg, os resultados foram melhores para os testes realizados com QoS e o LFI habilitado fim a fim. Alguns parâmetros de QoS testados conforme a tabela acima mostra que os resultados foram satisfatórios comparativamente com os resultados dos testes sem QoS e sem LFI habilitado apesar do tempo de teste ter sido doze vezes menor. Nesta mesma Tabela 8, tem-se discriminado a leitura dos parâmetros como o jitter, percentual de descartes de pacotes, banda consumida.
- que tendo em conta que a rede usada - Frame Relay, a LFI - depende de uma prévia configuração de QoS, independentemente das suas políticas de entrada e ou saída das interfaces dos roteadores levou a que haja um incumprimento de um dos parâmetros do FRTS como por exemplo o CIR (Taxa média de dados por unidade de tempo) o que fez com que a qualidade do sinal de fala fosse degradada, dado que valores muito acima do CIR tornou a rede instável.
- que outro valor como a taxa de *pps* (pacotes por segundos) bem como o tamanho de pacotes, ficou nitidamente evidenciado nos testes que devem sempre ser devidamente mensurados a fim de garantir QoS fim-a-fim;
- que ocorria perda de pacotes de forma indiscriminada, quando não se teve o cuidado de gerenciar adequadamente a banda, resultando em taxas de perda na

ordem de 58 %, mesmo para tráfegos classificados como sendo classes prioritárias, e, além disso, percebeu-se o elevado valor do *delay* tanto para valor mínimo como médio e o máximo *delay* registrado; jitter de 2,722 sec, contrariando as normas padronizadas;

- que sem a implementação de QoS, pacotes sofreriam perda indiscriminadamente, principalmente se os parâmetros FRTS não forem respeitados em algum momento e que com QoS preservou-se a integridade dos pacotes marcados como prioritários independentemente do tamanho dos demais fluxos que disputavam a banda em paralelo;
- que quando foi testado o nível de “saturação” / congestionamento do link percebeu-se que o congestionamento inviabilizou as aplicações independentemente das suas classificações e com a LFI habilitada e ou tendo ela desabilitada. O critério usado para testar congestionamento foi necessariamente a violação de alguns parâmetros do FRTS. Por outro lado, percebeu-se também que tráfegos com baixos valores e ou nos limites dos parâmetros de FRTS fluem normalmente;
- que usando Acterna e os dois ramais pacotes *ftp* acima da MTU relacionando os quadros de voz em um ambiente sem QoS, tornou impraticável a pratica de conversa telefônica e a não LFI provocou altos delay, atraso de serialização dos frames de voz na entrada da interface; altos jitter, causando perda e falhas na recepção da aplicação;
- que com a intercalação dos frames de voz - fluxos RTP, classe voz, marcação – EF, sempre receberam preferência na alocação de banda entre os demais frames da classe *Business* - marcação AF31 e obteve-se como resultados, baixos delay, jitter toleráveis, devido ao não atraso de serialização dos pacotes *ftp* e sem perda;

Estes resultados apresentados nesta seção são incompletos, ou seja, não são resultados finais. São, portanto, os resultados pré-liminares que permitirão o bom entendimento dos resultados complementares, que serão apresentados no capítulo VI seguinte.

6 - CAPÍTULO VI: MEDIÇÕES COMPLEMENTARES COM TRÁFEGOS DE DIFERENTES CODECS

*“A teoria sempre acaba, mais cedo ou mais tarde,
assassinada pela experiência”
- Albert Einstein*

Neste capítulo, estão relacionados todos os testes mais complexos, ou seja, nos testes ditos complementares são manipulados diversos parâmetros de melhoria de desempenho de redes. Esses testes foram levados a cabo, correlacionando diversas técnicas em um mesmo tráfego envolvendo, por exemplo, compressão de cabeçalho, LFI, QoS, alternando os codecs e repetindo os testes, por exemplo, sem compressão e sem a FLI, etc.

6.1 – Objetivo das medições correlacionando LFI, QoS, cRTP e CODECs em um mesmo tráfego.

Nesta seção é exibida uma série de resultados de medições onde são correlacionados parâmetros como QoS, LFI, cRTP e três tipos de codecs de voz diferentes, a fim de se avaliar o seguinte:

- ✓ O desempenho das aplicações e a sua viabilidade;
- ✓ Comportamento da rede, por exemplo, no quesito ocupação de banda;
- ✓ Análise sobre a ocupação da banda por cada teste;
- ✓ Análise de viabilidade de codec;
- ✓ Otimização do enlace com compressão RTP;
- ✓ Quantidades de canais de voz a serem adicionados quando for comprimido RTP;
- ✓ Perda de pacotes;
- ✓ Jitter, etc.

Neste sentido, são realizadas, pelo menos, quatro tipos de medições distintas e importantes com alternância do tipo de codec, tamanho de fragmento e habilitação ou desabilitação de compressão de cabeçalho RTP. Assim sendo, seguem os testes conforme descrito a seguir.

6.1.1 - Porquê estes testes

Estes testes têm como objetivo principal avaliar a viabilidade de aplicações VoIP em enlace de baixa capacidade, com o mínimo de banda reservada para aplicação VoIP em tráfegos paralelos, com aplicações do tipo dados. São, igualmente, manipulados pelo menos três parâmetros de melhoria de desempenho das aplicações e otimização de enlace:

- ✓ Três tipos de codecs distintos – G711, G729 e G726;
- ✓ Implementação de QoS ou não implementação de QoS;
- ✓ Habilitação de compressão RTP ou a não habilitação da compressão RTP;
- ✓ Habilitação da LFI ou a não habilitação da LFI.

6.1.2 - Metodologia de desenvolvimento dos testes

Para realizar os testes segundo a Seção 4.1.1 - "O que testar e quais testes fazer" do capítulo IV, da alínea (9) foi criada e seguida a metodologia baseada na caracterização de perfis de tráfegos para cada aplicação retratada nas matrizes correspondentes como o caso da matriz da Tabela 10 a seguir. Nessas matrizes serão correlacionados todos os parâmetros e políticas necessários para a realização dos referidos testes. São discriminados os tipos de filas bem como seus algoritmos de escalonamento, tamanhos de banda reservada, tipo de codec por teste, tamanho de *payload*, etc.

6.1.3 – Caracterização de perfil de tráfegos nas medições sem QoS, sem LFI, sem cRTP, com os Codecs g729,g726,g711.

A matriz (Tabela 10) relaciona as três classes de serviços de rede para a banda total de 512kbps, com as características do perfil de tráfego de cada aplicação e os respectivos protocolos da rede e utilizados. Percebe-se na Tabela 10 - que todos os tráfegos são tratados de igual forma na fila, não há habilitação da LFI, nem marcação de pacotes.

Desta forma analisa-se a caracterização do tráfego de acordo com a Tabela 10 - a seguir:

Caracterização dos Perfis de QoS dos Tráfegos nos CPE's (Sem políticas QoS, Sem cRTP, sem LFI, testados com Três codecs diferentes)																	
		BANDA Reservada (Kbps)	Tipo Codec	Payload em Bytes Sem Cabeçalho	Pacotes/ sec (pps)	Duração/ período	Tipo de taxa Transmissão	Tipo Protocolo	Uso de LFI	Uso de cRTP	Qdes Fila/ Fluxo	DLCI	Tipo de Marcação	CIR/ minCIR (Kbps)	BC/BE (bytes)	Tipo FILA	Burst (bytes)
CoS	Rede	512	x	x	x	x	x	x	x	x	x	100	x	521	6144 /0	FIFO	1500
1	Voz *	60	G729	20	50	120sec	CBR	RTP / Frame Relay	x	NÃO	1	x	NÃO	x	x	FIFO	1500
		52	G726	80	50												
		82	G711	160	50												
2	Ftp	400	x	1000	50	10 sec	Periodica	UDP	NÃO	NÃO	1	x	NÃO	x	x	FIFO	X
3	Default	30	...	x	50	x	Periodica	UDP	x	x	(Hashed Queues)	X	X	X	X	FIFO	X
											32						
OBS: * A classe um (1) voz, tem a banda reservada de acordo com o codec a ser utilizado																	

Tabela 10 - Caracterização dos Perfis de QoS dos Tráfegos nos CPE's (Sem políticas QoS, Sem cRTP, sem LFI, testados com Três codecs diferentes)

A Tabela 10 ilustra as três classes de serviços seguintes: voz, ftp e a default. Estas três classes receberam do total de banda de acesso frame Relay 512kbps, estando reservadas as seguintes quotas de bandas: Dados FTP = 400kbps, classe Default = 30kbps e Frames de voz = 60kbps caso for usado codec de voz G729. Se, se usar outros codecs tal como o G711 a banda para classe voz seria de 82kbps, 52kbps ou 60kbps para o codec G726, pois, segundo dizem as recomendações, banda inferior comprometeria a viabilidade da aplicação de tempo real com voz interativa.

Na mesma Tabela 10 pode-se ainda perceber do número de pacotes por segundos gerados (nesse caso 50pps) a todas as aplicações; payload de cada aplicação; tempo de reprodução ou periodicidade de reprodução, bem como o tipo de transmissão, tipo de protocolo a ser usado por cada aplicação. Ainda ficou evidente o não uso da compressão, marcação de pacotes, algoritmo utilizado para implementar a fila, parâmetros de modelagem de trafego em Frame Relay como CIR, BE, entre outros parâmetros. Mostra também a tabela acima a quantidade de trafego por classe – 1 (um) tráfego de tempo real e 1 (um) tráfego FTP.

6.1.3.1 - Resultados dos testes e as suas respectivas interpretações

Como parte de resultados analisados, foi filtrado através do script do CEP03 cuja interface origem 192.168.0.10 a destino 192.168.0.6 de acesso ao Frame Relay os

30 últimos segundo de taxa de ocupação de banda, conforme a Tabela 40 - Ocupação da Banda da medição Sem QoS, Sem cRTP, sem LFI, codec G729 (Vide Apêndice I - Seção Acterna), permitindo montar a Tabela 11 a seguir.

Ocupação da Banda da medição Sem QoS, Sem cRTP, sem LFI, codec G729							
Partilha da Banda		Parametros entrada				Banda Ocupada	Percentual de Banda ocupada
Total	Reservada: Voz +Dados	Codec Usado	Payload d Voz (Bytes)	Pacotes FTP (bytes)	Taxa (pps)	Estatística dos 30 'Ultimos Sec em (kbps)	Banda Total :: Banda Reservada
512kbps	460bytes	G729	20 bytes	1000 bytes	50pps	449,6kbps	87,82% :: 97.74%

Tabela 11 - Medição da banda Sem QoS, Sem cRTP, sem LFI, codec G729

O Roteador Cisco permite a coleta dos últimos 30 segundos dos tráfegos das aplicações. Com o VAD desabilitado o Roteador Cisco gera pacotes a taxa constante de 50pps (pacotes por segundos). Assim usando o codec G729, a ocupação de banda foi de 449600bits por segundos, ou seja, de 449kbps. Isso leva-nos a entender que esse valor em algum momento estourou o limite máximo de 400kbps de dados reservado. Entretanto, como havia uma reserva de 60 kbps de classe voz, esse valor ficou praticamente no limiar da banda reservada uma vez que os pacotes foram gerados durante 120sec a taxa de reprodução de 50pps e pacotes de 20bytes e 1000bytes para voz e dados respectivamente.

Conclui-se, então, que as duas aplicações tiveram um consumo da banda em termos percentuais de 87,82% em relação a banda total (512kbps) e 97,74% em relação a banda reservada para as duas aplicações, pois essas aplicações não receberam tratamentos como a Compressão RTP.

Para se entender melhor a análise dos resultados extraídos com relação ao jitter para as aplicações de voz, Tabela 12 a seguir ilustra de fato como foi o comportamento das aplicações, analisando os seus respectivos valor de jitter.

A Tabela 12 a seguir de uma forma geral dá essa idéia da variação do jitter em termos de valores medianos para cada CODEC.

JITTER MEDICOES SEM LFI, SEM QoS E SEM cRTP LFI- 1500	G711	G726	G729
JITTER (ms) - Minimo	19,92	23,24	15,40

Tabela 12 - Valores de Jitter dos testes Sem políticas QoS, Sem cRTP, sem LFI, testados com Três codecs diferentes.

A Tabela 12 ainda diz-nos que o melhor valor mínimo de variação de atraso é de 15.40ms para um tráfego usando o codec G729, sendo que os outros dois valores estão no limiar – limite de 20ms e acima desse valor com jitter Maximo de 96,5ms essa variação é contra-indicado; entretanto para outros codecs estão valores acima de 15,40ms. Registrado jitter de 23,24 para tráfego usando o codec G726 . Entretanto, durante os testes, usando os ramais telefônicos pode perceber que foi inviável tal prática de telefonia, uma vez que a ligação era bastante perturbadora, com altos picos de interrupções e cortes.

Ainda de acordo com a Tabela 12, apesar do jitter de 15.40ms estar dentro do limite aconselhável, não foi um caso de sucesso durante os dois minutos (120sec) de conversa telefônica usando os ramais R3000 a R5000 ilustrados pela Figura 20 a seguir.

Figura 20- Medição Sem QoS e Sem LFI G729 e Sem cRTP

Não houve fragmentação do pacote de dados nem compressão de cabeçalho. A ligação foi, entretanto, com picos de cortes, pois a variação de atraso fora imprevisível, chegando a 96,5ms e ora a 1,1ms, na havia qualquer linearidade entre essa variação do atraso.

A Figura 21 a seguir, segue as mesmas configurações ilustradas na Tabela 10, segue as mesmas descrições que a Figura 20, com algumas alterações no quesito tamanho do payload, variação do atraso, codec utilizado.

Frame Relay	Size	IP	Destination	UDP	RTP	Source	Interpretation
1.1 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
14.0 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
16.5 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
91.1 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
1.1 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
6.1 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
28.1 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
20.2 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
50.0 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
20.1 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
18.8 ms	126	192.168.0.10	192.168.0.6	RTP	G.726	Audio	
14.7 ms	1034	10.30.0.2	10.20.0.2	UDP	D=COMPLEX LIN		
2.8 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
37.0 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
3.5 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
20.0 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
20.0 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
28.4 ms	126	192.168.0.10	192.168.0.6	RTP	G.726	Audio	
16.2 ms	1034	10.30.0.2	10.20.0.2	UDP	D=COMPLEX LIN		
91.3 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
14.0 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
14.0 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
23.5 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
17.0 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
50.8 ms	126	192.168.0.10	192.168.0.6	RTP	G.726	Audio	
16.2 ms	1034	10.30.0.2	10.20.0.2	UDP	D=COMPLEX LIN		
1.4 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
14.0 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
1.1 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
7.8 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
96.5 ms	126	192.168.0.10	192.168.0.6	RTP	G.726	Audio	
16.2 ms	1034	10.30.0.2	10.20.0.2	UDP	D=COMPLEX LIN		
1.4 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
1.1 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
28.1 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
0.1 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
5.9 ms	166	192.168.0.10	192.168.0.10	RTCP	Source Description		
28.1 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
1.1 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
16.2 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	
50.0 ms	126	192.168.0.6	192.168.0.10	RTP	G.726	Audio	

Figura 21 - Medição Sem QoS e Sem LFI G726 e Sem cRTP

Contrariamente, a Figura 20, foi usado o codec G726, que por consequência exige que o tamanho do payload seja de 80bytes, que somado ao cabeçalho passa para 126bytes sem a compressão.

Percebe-se ainda na Figura 21, que os valores de jitter foram superiores aos do mesmo teste usando o codec G729. Sendo assim, infere-se, com base nesses valores, que o codec G729 oferece mais aderência a frames de voz comparativamente com G726.

Fora perceptível que em um dado momento surgiu uma sequência de jitter de 20-20-28,4-16,2-91,2-14. Isso implica dizer que além dos picos agudos nas ligações, essas sequências de variação de atrasos deixam a comunicação inviável, ou pelo menos, por alguns instantes de tempo os participantes não se entenderiam.

A Figura 22 - a seguir representa uma das ultimas series de três medições sem quaisquer políticas de QoS.

Frame Relay	IP	UDP	RTP	Interpretation
DeltaTime	Size	Destination	Source	
50.8 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
20.0 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
50.8 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
28.4 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
16.2 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
6.1 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
20.4 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
20.2 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
17.0 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
20.1 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
18.8 ms	206	192.168.0.10	192.168.0.6	RTP G.711 Audio Seq
1.5 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
14.7 ms	1034	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK
2.8 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
37.0 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
3.5 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
20.0 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
17.0 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
28.4 ms	206	192.168.0.10	192.168.0.6	RTP G.711 Audio Seq
16.2 ms	1034	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK
1.3 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
1.1 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
14.0 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
23.5 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
17.0 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
50.8 ms	206	192.168.0.10	192.168.0.6	RTP G.711 Audio Seq
16.2 ms	1034	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK
1.4 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
50.8 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
1.1 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
7.8 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
96.5 ms	206	192.168.0.10	192.168.0.6	RTP G.711 Audio Seq
16.2 ms	1034	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK
1.4 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
1.1 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
17.0 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
1.1 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
3.9 ms	166	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
1.1 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
50.8 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
16.2 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq
17.0 ms	206	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq

Figura 22 - Medição Sem QoS e Sem LFI G711 e Sem cRTP

A Figura 22, contrariamente as demais da serie, usa o codec G711, fazendo com que o *payload* do frame de voz seja de 206bytes sem a compressão RTP.

Contrariamente à Figura 21- anterior em que foi usado o codec G726, este foi usado o codec G711, que apesar de gerar frames com maior valor absoluto de *payload*, e jitter elevados muito similar os G726, este apresenta menos perturbações do que o G726 quando se escuta as conversações. Isso permite-nos concluir que o G711 possui melhor facilidade em lidar com o VoIP em relação ao G726, entretanto o G729 lidou melhor que os dois comparativamente, pois de uma forma geral o G729 permita maior compressão de áudio já codificado no codec.

O G729 reproduz a taxas mínimas de 8kbps e 10 frames por segundos, uma das qualidades que o diferencia das demais. Para se ter uma idéia gráfica das medições usando os três codecs diferentes, foi esboçado um gráfico de linhas que deixa

transparecer as oscilações dos fluxos em ondas contínuas conforme representada no gráfico (Figura 23) a seguir.

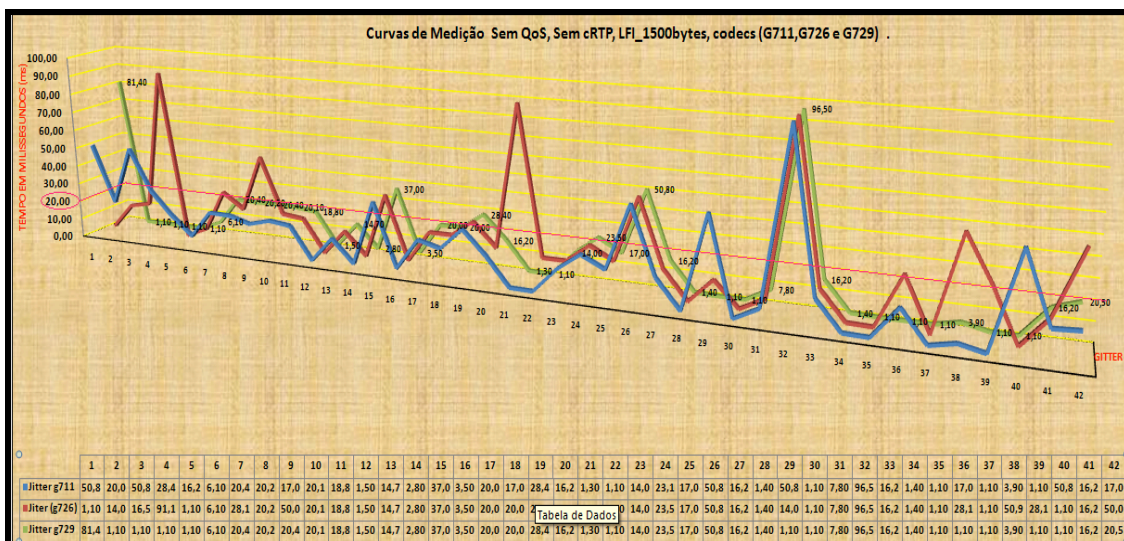


Figura 23 - Gráfico de Jitter dos testes Sem políticas QoS, Sem cRTP, sem LFI, testados com Três codecs diferentes

Na Figura-23 percebe-se um gráfico - relação tempo de valores de jitter aceitáveis, vezes os valores de jitter gerados têm-se uma linha da cor rosa, que representa o limiar aceitável para boas aplicações de real time como voz de 20ms. Percebe-se que uma boa parte de tempo as aplicações mantiveram abaixo ou no limite ou pouco acima desse limite, seriam as aplicações de voz e os altos picos referem aos pacotes de dados.

Esses pacotes de dados, entretanto, não são afetados pelos altos valores de jitter, pois dados do tipo FTP não são sensíveis ao atraso ou suas variações – *Jitter*. Neste gráfico, percebe-se que a linha destacada a cor verde, tem uma forma mais linear possível se comparada com as outras duas linhas. Esta linha de cor Verde representa o fluxo de voz gerada pelo codec G729.

6.1.4 - Caracterização do perfil de tráfegos nas medições com LFI habilitado a 640bytes de fragmento, com QoS, com cRTP desabilitado e usando os codecs g711,g726,g729

A matriz Tabela 13 - a seguir segue as mesmas definições que a matriz – Tabela 10. Esta, entretanto, apresenta algumas particularidades, já que se trata de uma matriz de caracterização de perfil de tráfego para perfil de QoS em que ocorre a implementação

de LFI com fragmento de tamanho máximo de 640bytes; os pacotes são devidamente marcados e as filas receberão tratamento adequadas.

Caracterização dos Perfis de QoS dos Tráfegos nos CPE's (Com políticas QoS, Sem cRTP, com LFI-640bytes, testados com Três codecs diferentes)																	
		BANDA Reservada (Kbps)	Tipo Codec	Payload em Bytes Sem Cabeçalho	Pacotes/ sec (pps)	Duração/ período	Tipo de taxa Transmissão	Tipo Protocolo	Uso de LFI	Uso de cRTP	Qdes de Fila/ Fluxo	DLCI	Tipo de Marcação	CIR/ minCIR (Kbps)	BC/BE (bytes)	Tipo FILA	Burst (bytes)
CoS	Rede	512	x	x	x	x	x	x	x	x	x	100	x	521	6144 /0	FIFO	1500
1	Voz *	60	G729	20	50	120sec	CBR	RTP / Frame Relay	x	NÃO	1	x	EF	x	x	Strict Priority	1500
		52	G726	80	50												
		82	G711	160	50												
2	Ftp	400	x	1000	50	10 sec	Periodica	UDP	640	NÃO	1	x	AF31	x	x	Fair Queue	X
3	Default	30	...	x	50	x	Periodica	UDP	x	x	(Hashed Queues) 32	X	X	X	X	FIFO	X
OBS: * A classe um (1) voz, tem a banda reservada de acordo com o codec a ser utilizado																	

Tabela 13 - Caracterização dos Perfis de QoS dos Tráfegos nos CPE's (Com políticas QoS, Sem cRTP, com LFI-640bytes, testados com Três codecs diferentes)

Percebe-se na tabela (Tabela 13) anterior que, ao contrário da outra implementação que não previa qualquer tipo de QoS esta prevê. Esta tabela prevê implementação de QoS, habilitação de LFI, porém, não prevê a compressão de cabeçalho. Deste modo, foram marcadas as classes serviços Voz e business para EF e AF31 respectivamente, e as mesmas receberam também as seguintes implementações das filas de QoS como *Strict Priority* e *Fair Queue* respectivamente, a classe default recebeu a fila FIFO.

Foram usados os seguintes codecs para cada um dos testes: G711, G726 e G729, entretanto, para fins de marcação de ocupação da banda, foi tomado como referencia o codec G729. Os resultados desses testes seguem na próxima seção.

6.1.4.1 - Resultados dos testes e as respectivas interpretações

A Tabela 14 - a seguir ilustra o quanto de banda foi usado neste teste.

Banda ocupada na medição com QoS, Sem cRTP, com LFI-640bytes, G729							
Partilha da Banda		Parametros entrada				Banda Ocupada	Percentual de Banda ocupada
Total	Reservada: Voz +Dados	Codec Usado	Payload d Voz (Bytes)	Pacotes FTP (bytes)	Taxa (pps)	Estatistica dos 30 'Ultimos Sec em (kbps)	Banda Total :: Banda Reservada
512kbps	460bytes	G729	20 bytes	1000 bytes	50pps	403,6kbps	78,83% :: 87,74%

Tabela 14 - Banda ocupada na medição com QoS, Sem cRTP, com LFI-540bytes, G729

Na matriz (Tabela 14) pode ser percebido que apesar de não ter sido habilitada a compressão de cabeçalho, a ocupação de banda nos últimos 30 segundos a 50pps foi tecnicamente menor de 403,6kbps. Essa redução de consumo de banda está relacionada ao fato de que os fluxos receberam tratamento específico e fluíram com mais rapidez sem que um atrapalhasse o outro.

Comparativamente a Tabela 11 - resultado dos testes sem LFI, sem QoS e sem compressão usando igualmente o codec G729, esta com LFI, com QoS e também sem compressão apresenta uma vantagem de economia de banda na ordem de 449600bps para 403600bps o que representa em termos de percentagem um ganho de aproximadamente de 11%.

Conclui-se, portanto, que as duas aplicações voz e Dados (FTP), ocuparam 78,83% da banda total (512kbps) e 87,74% da banda reservada para as duas aplicações (460kbps).

Em termos de variação do atraso, foi contrariamente ao outro modelo, dentro os limites aceitáveis do 20ms, com apenas alguns picos, sendo assim a Tabela 15 - a seguir mostra essa variação de atraso em termos de valores medianos para cada codecs aplicando QoS e LFI.

JITTER MEDICOES COM LFI, COM QoS, COM cRTP LFI- 640Bytes	G711	G726	G729
Média Jitter (ms)	8,72	10,62	5,96

Tabela 15 - Valores de Jitter de testes Com políticas QoS, Sem cRTP, com LFI-640bytes, testados com Três codecs diferentes

A Tabela 15 - mostra a relação da variação do tempo entre três tipos de codecs e as aplicações quando foram aplicados QoS, LFI e foram comprimidos os cabeçalhos. Se observados os valores medianos de todos os fluxos sem analisar a variação dos fluxos um a um, conclui-se que foi um caso ótimo, pois todos os valores de *jitter* estão abaixo do limiar recomendado.

Todos os codecs deram suporte adequado, entretanto o G729 continua sendo o melhor logo em seguida o G711 e na sequência o G726 com diferenças mínimas se comparado ao G711. Na medição com QoS configurada e LFI habilitada sem compressão RTP usando o codec G729, o maior jitter para aplicação de voz foi de 5,9ms e o menor foi de 220microsec, e o maior jitter para aplicação de dados foi de 16,2 conforme a Figura 14 - a seguir.

Delta Time	Size	Destination	Source	Interpretation
5.6 ms	66	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=370 Timestamp=154
8.1 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
6.3 ms	398	DCE	DTE	Frame Relay DCE=100 InformationLink=2
5.6 ms	66	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=371 Timestamp=154
8.1 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
5.9 ms	66	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=372 Timestamp=154
420 us	398	DCE	DTE	Frame Relay DCE=100 InformationLink=2
11.0 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
6.3 ms	398	DCE	DTE	Frame Relay DCE=100 InformationLink=2
220 us	66	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=373 Timestamp=154
16.2 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
3.9 ms	66	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=374 Timestamp=154
2.4 ms	398	DCE	DTE	Frame Relay DCE=100 InformationLink=2
13.7 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
4.4 ms	66	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=375 Timestamp=154
1.9 ms	398	DCE	DTE	Frame Relay DCE=100 InformationLink=2
13.7 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
4.4 ms	66	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=376 Timestamp=154
1.9 ms	398	DCE	DTE	Frame Relay DCE=100 InformationLink=2
13.7 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
4.9 ms	66	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=377 Timestamp=154
1.4 ms	398	DCE	DTE	Frame Relay DCE=100 InformationLink=2
13.9 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
4.7 ms	66	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=378 Timestamp=154
1.6 ms	398	DCE	DTE	Frame Relay DCE=100 InformationLink=2
9.9 ms	157	192.168.0.6	192.168.0.10	H.225.0 CONNECT IRI=Bearer Capability
3.6 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
5.4 ms	66	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=379 Timestamp=154
900 us	398	DCE	DTE	Frame Relay DCE=100 InformationLink=2
13.8 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
5.5 ms	66	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=380 Timestamp=154
800 us	398	DCE	DTE	Frame Relay DCE=100 InformationLink=2
1.1 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=5612 Timestamp=21
12.6 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
3.6 ms	66	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=5613 Timestamp=21
290 us	398	DCE	DTE	Frame Relay DCE=100 InformationLink=2
1.1 ms	66	192.168.0.10	10.20.0.2	RTP G.729 Audio Seq=5614 Timestamp=21
10.2 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
6.3 ms	398	DCE	DTE	Frame Relay DCE=100 InformationLink=2
1.1 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=5615 Timestamp=21
1.5 ms	66	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=383 Timestamp=154
14.1 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
5.9 ms	66	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=384 Timestamp=154

Figura 24 - Medição Com QoS e Com LFI G729 e Sem cRTP

Com essas amostras fica claro que os serviços de tempo real não foram atrapalhados, pois intercalação dos frames de voz em pacotes de dados foi habilitada.

A Figura 25 - a seguir representa o comportamento dos fluxos para cada tráfego, que são identificados pelos protocolos de comunicação, endereços de origem e destino, variação do atraso, e tamanho do frame, dentre outras características.

DeltaTime	Size	Destination	Source	Interpretation
20.6 ms	126	192.168.0.6	192.168.0.10	RTP G.726 Audio Se
8.1 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LIN
6.3 ms	398	DCE	DTE	Frame Relay DICI=1
17.3 ms	126	192.168.0.6	192.168.0.10	RTP G.726 Audio Se
8.1 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LIN
17.9 ms	126	192.168.0.6	192.168.0.10	RTP G.726 Audio Se
420 us	398	DCE	DTE	Frame Relay DICI=1
14.4 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LIN
1.1 ms	398	DCE	DTE	Frame Relay DICI=1
720 us	126	192.168.0.6	192.168.0.10	RTP G.726 Audio Se
16.2 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LIN
3.9 ms	126	192.168.0.6	192.168.0.10	RTP G.726 Audio Se
8.4 ms	398	DCE	DTE	Frame Relay DICI=1
13.7 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LIN
19.4 ms	126	192.168.0.6	192.168.0.10	RTP G.726 Audio Se
20.9 ms	398	DCE	DTE	Frame Relay DICI=1
13.7 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LIN
4.4 ms	126	192.168.0.6	192.168.0.10	RTP G.726 Audio Se
17.9 ms	398	DCE	DTE	Frame Relay DICI=1
8.7 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LIN
4.9 ms	126	192.168.0.6	192.168.0.10	RTP G.726 Audio Se
1.4 ms	398	DCE	DTE	Frame Relay DICI=1
13.9 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LIN
10.7 ms	126	192.168.0.6	192.168.0.10	RTP G.726 Audio Se
20.6 ms	398	DCE	DTE	Frame Relay DICI=1
10.3 ms	157	192.168.0.6	192.168.0.10	H.225.0 CONNECT IE
3.6 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LIN
19.4 ms	126	192.168.0.6	192.168.0.10	RTP G.726 Audio Se
900 us	398	DCE	DTE	Frame Relay DICI=1
16.8 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LIN
17.5 ms	126	192.168.0.6	192.168.0.10	RTP G.726 Audio Se
1.1 ms	398	DCE	DTE	Frame Relay DICI=1
20.1 ms	126	192.168.0.10	192.168.0.6	RTP G.726 Audio Se
12.6 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LIN
17.9 ms	126	192.168.0.6	192.168.0.10	RTP G.726 Audio Se
1.4 ms	398	DCE	DTE	Frame Relay DICI=1
19.1 ms	126	192.168.0.10	192.168.0.6	RTP G.726 Audio Se
1.1 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LIN
20.0 ms	126	192.168.0.6	192.168.0.10	RTP G.726 Audio Se
800 us	398	DCE	DTE	Frame Relay DICI=1
8.1 ms	126	192.168.0.10	192.168.0.6	RTP G.726 Audio Se
10.2 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LIN
6.3 ms	126	DCE	DTE	Frame Relay DICI=1
1.1 ms	126	192.168.0.10	192.168.0.6	RTP G.726 Audio Se
19.5 ms	126	192.168.0.6	192.168.0.10	RTP G.726 Audio Se
20.1 ms	648	10.30.0.2	10.20.0.2	UDP D-COMPLEX LIN
800 us	126	192.168.0.6	192.168.0.10	RTP G.726 Audio Se

Figura 25 - Medição Com QoS e Com LFI G726 e Sem cRTP

Como foi usado o codec G726 sem compressão os pacotes de payload de voz assumem o tamanho de 126bytes por fluxos que foram sucessivamente intercalados entre os pacotes de dados.

Esses pacotes de dados sofreram fragmentação a fim de prover a intercalação dos pacotes de voz e evitando que esperassem por muito tempo na fila caso os pacotes de dados fossem enviados antes dos frames de voz. Esse atraso de serialização na espera para envio dos frames de voz por períodos acima do recomendado, causaria um atraso que desfavorece a viabilidade da comunicação de tempo real.

O G726, embora apresentasse o codec menos desfavorecido nas medições anteriores, esta agora apresentou ser razoável em termos de jitter, embora ainda perca em termos de ocupação de banda. Da coluna de variação de atraso (*DeltaTime*) percebe-se que os valores do jitter são mais elevados de uma forma geral se comparado a análise em que foi usado o codec G729, pois existem picos de jitter na ordem de 20,6 ms enquanto o limite aconselhável é de 20 ms. Esse pico de 20,6ms ainda pode ser considerado tolerável, já que durante as conversações foi possível entender a outra parte Ramal 5000 e vice versa (ramal 3000) ainda que com essas pequenas elevações de picos. Na sequência desses conjuntos testes e medições, falta para essa seção medir os mesmos parâmetros e mesmos serviços alternando o tipo de codec, sendo assim, a Figura 26 a seguir ilustra as medições a partir do uso do codec G711.

Os resultados de análise de jitter estão associados ao codec G711, que faz com que os pacotes de voz sejam gerados a tamanhos de 206bytes já incluindo todos os cabeçalhos.

Curvas de Medição com QoS, com LFI_640, e Sem cRTP, com codecs (G711, G726 e G729)

ExoHorizontal (Categoria)

JITTER

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
GITTER (G729)	5,60	8,10	6,30	5,60	8,10	5,90	0,42	11,00	6,30	0,22	16,00	3,60	1,40	9,70	0,40	1,90	13,90	4,40	1,80	9,30	1,60	9,90	1,40	5,40	13,40	5,90	9,70	1,10	0,30	5,40	9,70	1,10	0,10	11,60	6,30	0,10	12,60	6,00	0,20	10,20	6,30	1,10	1,10	1,50	5,90		
GITTER (G711)	10,6	8,10	6,30	17,3	8,10	17,9	7,90	14,4	6,30	0,95	16,2	3,90	0,42	13,7	4,40	1,90	13,7	0,80	17,9	13,7	4,90	1,14	13,9	10,7	1,60	10,3	3,60	19,4	0,90	13,8	17,5	3,60	11,0	12,0	5,90	1,40	11,0	12,6	6,00	0,90	11,0	10,2	6,30	1,10	19,5	14,1	5,9
GITTER (G726)	20,6	8,10	6,30	17,3	8,10	17,9	0,42	14,4	1,10	0,72	16,2	3,90	8,40	13,7	16,4	20,9	13,7	4,40	17,9	8,70	4,90	1,40	13,9	10,7	20,6	10,3	3,60	19,4	0,90	16,8	17,5	1,10	20,1	12,6	17,9	1,40	19,1	11,0	20,0	0,80	8,10	10,2	6,30	1,10	19,5	20,1	8

Figura 27 – Gráfico de representação de variação do atraso para testes Com políticas QoS, Sem cRTP, com LFI-640bytes, testados com Três codecs diferentes

O gráfico (Figura 27) representa o jitter dos tráfegos fluxo a fluxo. As aplicações tiveram um bom comportamento, na sua maioria, dentro do limite dos 20ms (sobressaído na linha horizontal de cor vermelha), apresentando assim, uma linearidade quase uniforme dos fluxos, conforme se pode observar na representação gráfica de linhas. Conforme foi dito anteriormente, os fluxos com picos de variações de atraso mais salientes são os fluxos gerados pelos codecs G726. De uma forma geral, considera-se, pelo resultado de medições, que os três diferentes testes entre si são aceites como sendo bons.

6.1.5 - Caracterização de perfis de tráfegos nas medição com QoS, com cRTP, LFI habilitado, usando o codec g729, com dois fluxos ftp concorrentes.

Nesta seção, as medições são diferentes, pois podem ser verificados conforme a caracterização do perfil do tráfego para um tráfego de tempo real (voz) entre os participantes 192.168.0.6 a 192.168.0.10, ramais 4000 a 6000, os dados (FTP), são provenientes da mesma fonte 10.20.0.2 para destinos diferentes IP 10.10.0.2 e 10.30.0.2. A matriz da Tabela 16 a seguir representa as demais informações que caracterizam o perfil do tráfego para esta bancada de teste.

Percebe-se que foi usado apenas o codec G729, pois, este ao longo dos testes apresentou melhor viabilidade e a banda reservada para classe voz continua sendo de 60kbps. Essa banda de 60kbps já está com uma folga de mais de 30%, pois, usando o G729 seria necessária uma reserva de 31,2kbps para ethernet e 26,8 para enlace frame relay fórum v12. Dado isso foi realocada a banda para a classe default a 52 Kbps.

O tamanho de fragmento, contrariamente aos demais testes, foi setado para 540 bytes, embora o valor máximo recomendado seja 640bytes para um link de 512kbps. Os equipamentos cisco aceitam esta configuração a menor, sem causar problema para a transmissão de dados.

Caracterização dos Perfis de QoS dos Tráfegos nos CPE's (1 Fluxo real time (Voz) e 2 tráfegos Ftp concorrentes)																	
		BANDA Reservada (Kbps)	Tipo Codec	Payload em Bytes Sem Cabeçalho	Pacotes/sec (pps)	Duração/ periodo	Tipo de taxa Transmissão	Tipo Protocolo	Uso de LFI	Uso de cRTP	Qdes Fila/ Fluxo	DLCI	Tipo de Marcação	CIR/ minCIR (Kbps)	BC/BE (bytes)	Tipo FILA	Burst (bytes)
CoS	Rede	512	x	x	x	x	x	x	x	x	x	100	x	521	6144 /0	FIFO	1500
1	Voz	60	G729	20	50	120sec	CBR	RTP / Frame Relay	x	SIM	1	x	EF	x	x	Strict Priorit y	1500
		X	G726	X	X												
		X	G711	X	X												
2	Ftp	400	x	1000	30	10 sec	Periodica	UDP	540	SIM	2	x	AF31	x	x	Fair Queue	X
3	Default	52	...	x	50	x	Periodica	UDP	x	x	(Hashed Queues) 32	X	X	X	X	FIFO	X

Tabela 16 - Caracterização dos Perfis de QoS dos Tráfegos nos CPE's (1 Fluxo real time (Voz) e 2 tráfegos Ftp concorrentes)

Na matriz Tabela 16, conforme anteriormente dito, são gerados dois tráfegos de dados usando o protocolo UDP em duas filas AF31 de algoritmo de escalonamento de filas *Fair Queue*. Cada um desses pacotes é fragmentado a 540 bytes no máximo, em intervalos periódicos de 10sec, a uma taxa fixa de 30pps.

6.1.5.1 - Resultados dos testes e as suas respectivas interpretações

Ao aferir-se os cálculos da ocupação da banda, verifica-se que esses ultrapassam em muito a banda reservada, sendo assim, o *script* do CPE, permitiu a coleta dessas estatísticas dos últimos 30sec permitindo montar a Tabela 17 a seguir.

Ocupação da Banda para testes Com políticas QoS, com cRTP, com LFI-540bytes, testados com codecs G729 e dois tráfegos FTP e um fluxo de voz									
Partilha da Banda		Alguns Parametros De Entrada						Banda Ocupada	Percentual de Banda ocupada
Total	Reservada: Voz +Dados	Clase Voz			Classe Business (FTP)			Estatística dos 30 'Ultimos Sec (kbps)	Banda Total :: Banda Reservada
		Codec Usado	Payload (Bytes)	Taxa (pps)	Pacotes (bytes)	Quantida de Trafego	Taxa (pps)		
512kbps	460bytes	G729	20 bytes	50pps	1000 bytes	2	30pps	506kbps	98,83% ::110%

Tabela 17 - Ocupação da Banda para testes Com políticas QoS, com cRTP, com LFI-540bytes, testados com codecs G729 e dois tráfegos FTP e um fluxo de voz.

Segundo a Tabela 17, em um link de capacidade máxima de 512kbps com dois tráfegos de dados de 1000bytes cada e, cada um deles a/em uma reprodução de 30pps adicionando o fluxo de tráfego de voz de um total de 66bytes a 50pps a 120sec, ultrapassar-se-ia em mais de 25% a capacidade do enlace total disponível. Como os pacotes sofreram compressão de cabeçalho, pode-se constatar que a ocupação da banda foi de 506kbps. Houve alguns descartes de pacotes na ordem de 2.15% e a rede ficou

saturada, a ponto de comprometer a viabilidade da aplicação de voz, embora havia já sido implementado o LFI, a compressão, pois a capacidade do enlace ficara seriamente comprometida.

Este caso, conforme era de se esperar, foi atípico, vendo as duas aplicações consumirem a banda na ordem de 98,83% em relação a banda total (512kbps) e 110% em relação a banda reservada para as duas aplicações, ou seja, a banda reservada ficou indisponível. Com relação ao jitter da rede e das aplicações, a Tabela 18 a seguir relaciona os valores em termos de valores médios do jitter da rede e das duas aplicações distintas, conforme o quadro que se segue:

JITTER de medições com QoS, com cRTP e LFI- 540Bytes - 2 tráfegos ftp e 1 fluxo de Voz	Todo tráfego da rede	FTP01	VOZ	FTP02
Média ponderada	37,46	19,86	5,70	11,84

Tabela 18 - Valores de Jitter para testes Com políticas QoS, com cRTP, com LFI-540bytes, testados com codecs G729 e dois tráfegos FTP e um fluxo de voz.

Da Tabela 18 infere-se que a rede comportou um jitter mediano de 37,46ms o tempo todo. Esse *jitter* não afetaria as aplicações FTP, mas tornar-se-ia inviáveis as aplicações VoIP, pois estes são sensíveis a altos valores de variação do atraso.. Da análise feita à tabela, percebe-se também o *jitter* para os dois tráfegos FTP e o tráfego de voz. O tráfego de voz teve um jitter mínimo de 5,70ms; com essa média pode-se dizer que a qualidade da conversação foi boa durante quase o tempo todo em que a mesma decorreu, não obstante ser considerável o valor de descarte de dados FTP e altos valores medianos para as aplicações FTP. Neste caso, a técnica que, de fato, colaborou para assegurar as aplicações de voz foi à habilitação de LFI.

Com a LFI habilitada os fragmentos introduzem menor valor de serialização aos pacotes de voz que esperam para serem intercalados. A Figura 28 a seguir, ilustra os fluxos um-a-um, para os dois tráfegos FTP e um de voz.

Dos valores sequenciais, percebe-se que os dados UDP e Frame Relay apresentaram maior *jitter* enquanto que os fluxos de voz apresentaram menor *jitter*, pois estes foram intercalados a datagramas de UDP e quadros Frame Relay e ainda sofreram compressão de cabeçalho e prioridade máxima na fila. Para uma melhor interpretação, o gráfico da Figura 29 - a seguir, representa as variações do jitter dessas aplicações, conforme se segue:

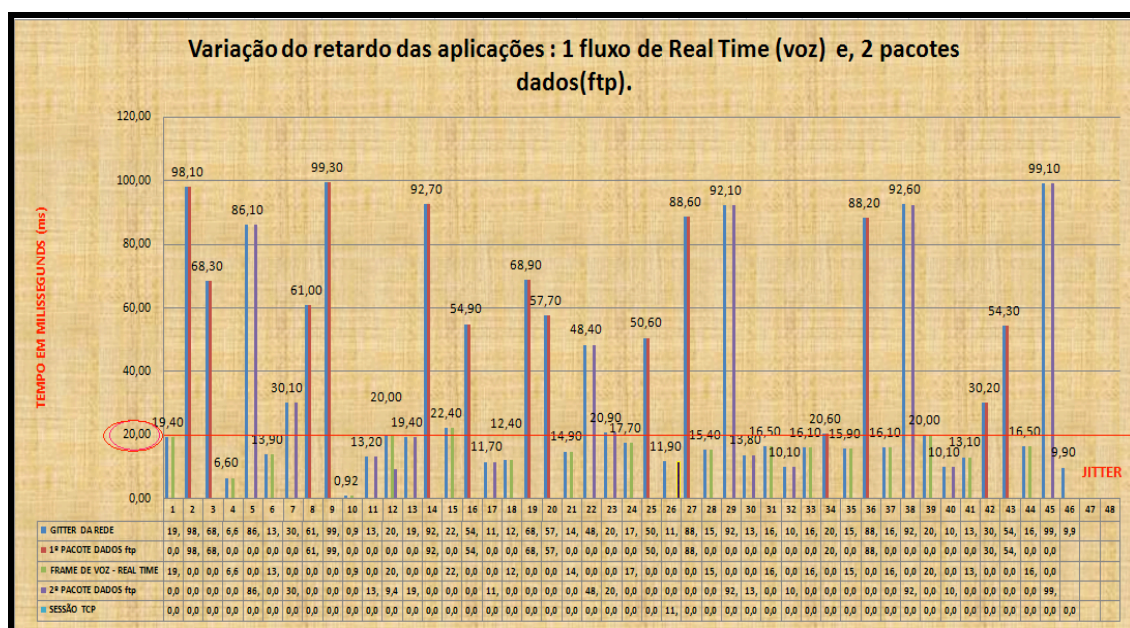


Figura 29 - Gráfico de representação de variação do atraso para testes Com políticas QoS, com cRTP, com LFI-540bytes, testados com codecs G729 e dois tráfegos FTP e um fluxo de voz.

Percebe-se, a partir do gráfico em apreço (Figura 29) que o tráfego de aplicação de voz (colunas verdes) manteve-se praticamente no limiar dos 20ms, conforme a linha delimitadora em cor vermelha horizontal. Dado que a rede foi muito sobrecarregada com os pacotes de dados FTP, apesar das políticas e mecanismos de QoS terem sido muito bem implementados, a conversação telefônica entre os dois ramais 4000 a 6000 apresentou picos constantes. Conclui-se ainda, com base nesse gráfico da Figura 29, que alguns desses picos chegaram a 22,4ms, valor muito acima do da recomendação ITU-T [35]. Esses picos deixariam a conversa embaraçada por alguns milissegundos, mas não inviabilizariam a aplicação no seu todo. Com isso, pode-se concluir que a associação das técnicas acima são viáveis e úteis.

6.1.6 - Caracterização de perfil de tráfegos nas medições com QoS negociada, com cRTP, com LFI, usando os codecs de voz g729, g726, g729 associado a um fluxo FTP.

A matriz da Tabela 19 a seguir representa um caso em que são colocados em paralelo um tráfego de dados FTP e um tráfego de voz. Seguindo as mesmas recomendações e especificações das medições da Tabela 16, foram testadas as referidas aplicações usando codecs diferentes conforme a Tabela 19. Os codecs G71, G726 e G729 são usados um de cada vez alternando-se entre os testes.

A Tabela 19 mostra os demais detalhes de caracterização de perfil de tráfego nos CPE's, usando compressão RTP, LFI a 540bytes e políticas de QoS negociadas implementadas.

Caracterização dos Perfis de QoS dos Tráfegos nos CPE's (Com políticas QoS, com cRTP, com LFI-540bytes, testados com Três codecs diferentes)																	
CoS	Rede	BANDA Reservada (Kbps)	Tipo Codec	Payload em Bytes Sem Cabeçalho	Pacotes/ sec (pps)	Duração/ período	Tipo de taxa Transmissão	Tipo Protocolo	Uso de LFI	Uso de cRTP	Qdes Fila/ Fluxo	DLCI	Tipo de Marcação	CIR/ minCIR (Kbps)	BC/BE (bytes)	Tipo FILA	Burst (bytes)
CoS	Rede	512	x	x	x	x	x	x	x	x	x	100	x	521	6144/0	FIFO	1500
1	Voz *	60	G729	20	50	120sec	CBR	RTP / Frame Relay	x	SIM	1	x	EF	x	x	Strict Priority	1500
		52	G726	80	50												
		82	G711	160	50												
2	Ftp	400	x	1000	50	10 sec	Periodica	UDP	540	SIM	1	x	AF31	x	x	Fair Queue	X
3	Default	30	...	x	50	x	Periodica	UDP	x	x	(Hashed Queues) 32	X	X	X	X	FIFO	X

OBS: * A classe um (1) voz, tem a banda reservada de acordo com o codec a ser utilizado

Tabela 19 - Caracterização dos Perfis de QoS dos Tráfegos nos CPE's (Com políticas QoS, Com cRTP, com LFI-540bytes, testados com Três codecs diferentes)

A Tabela 19 é, em parte, diferente da Tabela 16. Nesta matriz fora considerada a marcação do campo DSCP em pacotes de dados como AF31 e frame de voz com EF, o CIR de 521kbps, compressão de cabeçalho habilitado, *burst* (rajada) de 1500bytes equivalente ao máximo da MTU em quadros Ethernet, entre outras características necessárias para a garantia de uma boa provisão de QoS.

6.1.6.1 - Resultados dos testes e as suas respectivas interpretações

Das medições deduzidas dos perfis de tráfegos segundo a Tabela 19, pode ser analisada e comparada a ocupação de banda no enlace Frame Relay para cada um dos codecs analisados, conforme as tabelas seguintes (Tabela 20, Tabela 21, Tabela 22). Como são feitas medições usando os codecs G729, G726 e G711, especificamente para esses testes, pode-se fazer a análise de ocupação da banda em detrimento das medições conforme a Tabela 19 - anterior, começando pelo codec G729.

Ocupação da Banda para testes Com políticas QoS, com cRTP, com LFI, testados com codecs G729 um fluxo de voz e um tráfego FTP.							
Partilha da Banda		Parametros entrada				Banda Ocupada	Percentual de Banda ocupada
Total	Reservada: Voz +Dados	Codec Usado	Payload Voz (Bytes)	Pacotes FTP (bytes)	Taxa (pps)	Estatistica dos 30 'Ultimos Sec em (kbps)	Banda Total :: Banda Reservada
512kbps	460bytes	G729	20 bytes	1000 bytes	50pps	390,6kbps	76,29% :: 84,92%

Tabela 20 - Ocupação da Banda para testes Com políticas QoS, com cRTP, com LFI, testados com codecs G729 um fluxo de voz e um tráfego FTP.

Analisando a Tabela 20, verifica-se que a ocupação da banda usando o codec G729 nos últimos 30seg, com o VAD desabilitado, com taxa de reprodução a 50pps e com a compressão de cabeçalho habilitada, foi de 390,6 Kbps.

Conclui-se que este é o melhor resultado em termos de ocupação da banda, variação do atraso, viabilidade das aplicações, etc, pois, em termos de consumo da banda, as duas aplicações voz e ftp de 20bytes e 1000bytes, respectivamente, ocuparam 76,29% da banda total de 512kbps e 84,92% da banda reservada – 460kbps.

De forma semelhante, a Tabela 21 a seguir ilustra a ocupação da banda, em que as mesmas medições foram realizadas usando o codec G726, conforme, em seguida se pode verificar.

Ocupação da Banda para testes Com políticas QoS, com cRTP, com LFI testados com codecs G726 um fluxo de voz e um tráfego FTP							
Partilha da Banda		Parametros entrada				Banda Ocupada	Percentual de Banda ocupada
Total	Reservada: Voz +Dados	Codec Usado	Payload Voz (Bytes)	Pacotes FTP (bytes)	Taxa (pps)	Estatistica dos 30 'Ultimos Sec em (kbps)	Banda Total :: Banda Reservada
512kbps	452bytes	G726	80bytes	1000 bytes	50pps	400,35kbps	78,19% :: 88,57%

Tabela 21 - Ocupação da Banda para testes Com políticas QoS, com cRTP, com LFI-540bytes, testados com codecs G726 um fluxo de voz e um tráfego FTP

Na Tabela 21 observa-se a ocupação da banda passante da rede de 400,35kbps. Este valor é superior ao do dos mesmos testes utilizando o codec G729. Essa diferença em termos percentuais está em 2,50% da capacidade das duas aplicações. A banda reservada para a aplicação de voz foi 52bytes, ao invés de 60bytes. A banda de 60bytes reservada para voz usando o G729 foi sempre se 60kbps; para o G726 foi reservado 52kbps. Portanto, a banda reservada para as duas aplicações foi de 452kbps. Ademais, o tamanho do *payload* de voz para este codec é de 80bytes, valor esse 4 (quatro) vezes maior que o payload de codec G729. Com isso, fica claro que a rede terá mais consumo da banda do que o G729, devido a relação de 1 por 4 [5].

Comparando este resultado para os dois codecs G729 e G726, conclui-se que o G729 além de ser mais eficaz para aplicações VoIP, também ocupa menor capacidade de banda, pois o consumo efetivo da banda foi de 78,19% para o enlace total de 512kbps e 88,57% para o total da banda reservada para as duas aplicações.

A matriz da Tabela 22 a seguir mostra assim, o resultado da ocupação da banda para o codec G711, dado as mesmas configurações para as aplicações de voz e ftp.

Ocupação da Banda para testes Com políticas QoS, com cRTP, com LFI-540bytes, testados com codecs G711 um fluxo de voz e um tráfego FTP							
Partilha da Banda		Parametros entrada				Banda Ocupada	Percentual de Banda ocupada
Total	Reservada: Voz +Dados	Codec Usado	Payload Voz (Bytes)	Pacotes FTP (bytes)	Taxa (pps)	Estatistica dos 30 'Ultimos Sec em (kbps)	Banda Total :: Banda Reservada
512kbps	482bytes	G711	160bytes	1000 bytes	50pps	407,8kbps	79,65% ::84,61%

Tabela 22 - Ocupação da Banda para testes Com políticas QoS, com cRTP, com LFI-540bytes, testados com codecs G711 um fluxo de voz e um tráfego FTP

Na Tabela 22, registrou-se uma ocupação de banda na ordem de 407,8kbps. Esse valor de ocupação de banda é superior as outras duas medições usando o codec G726 e G729. Conclui-se que a medição feita usando o codec G711 ocupou, em termos

percentuais, mais banda que os demais na ordem de 1.83% em relação ao codec G726 e de 4,22% em relação ao codec G729. O G711 possui maior tamanho de payload 160bytes que representa um tamanho 8 (oito) vezes maior que o G729 e 2 (duas) vezes maior que o G726. O G711 requer, tecnicamente, maior banda se comparado aos demais [5],[33],[34].

O G711, apesar de ocupar mais banda, apresenta uma melhor viabilidade em relação ao G726 e uma ajustada compatibilidade de qualidade em relação ao codec G729.

A Tabela 23 a seguir mostra a relação entre os codecs utilizados e a variação do atraso para cada tráfego, em valores de *jitter* medianos para cada codec utilizado.

JITTER MEDICOES COM LFI, COM QoS, COM cRTP LFI- 540Bytes	G711	G726	G729
JITTER MEDIA	6,57	6,88	5,24

Tabela 23 - Valores de Jitter para testes Com políticas QoS, com cRTP, com LFI-540bytes, testados com um tráfego de voz usando os codecs G729, G711 e G726 e um tráfego FTP.

A Tabela 23, reforça a idéia de que os três codecs apresentam *jitter* em valores aproximados. A média dos valores é praticamente igual, embora se perceba, ainda, que o G729 apresenta uma melhor média, seguido do G711 e por último o G726.

O G711 apesar de possuir um maior tamanho de payload e ocupar maior capacidade de banda, comparado ao G726, demonstra melhor adequação e sensibilidade em lidar com aplicações VoIP.

A questão de análise de *jitter*, bem como o tamanho de cada *payload* comprimido podem ser analisados na Figura 30 a seguir que ilustra uma das telas geradas pelo Acterna Examine usando o codec G729 com LFI a 540bytes e com compressão RTP.

DeltaTime	Size	Destination	Source	Interpretation
3.6 ms	28	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=370 Timestamp=154
8.1 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
6.3 ms	498	DCE	DTE	Frame Relay DLCI=100 InformationType=
2.6 ms	28	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=371 Timestamp=154
8.1 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
5.9 ms	28	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=372 Timestamp=154
1.1 ms	498	DCE	DTE	Frame Relay DLCI=100 InformationType=
11.0 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
6.3 ms	498	DCE	DTE	Frame Relay DLCI=100 InformationType=
220 ms	28	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=373 Timestamp=154
13.2 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
3.9 ms	28	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=374 Timestamp=154
2.4 ms	498	DCE	DTE	Frame Relay DLCI=100 InformationType=
11.7 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
2.4 ms	28	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=375 Timestamp=154
1.9 ms	498	DCE	DTE	Frame Relay DLCI=100 InformationType=
11.7 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
2.4 ms	28	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=376 Timestamp=154
1.9 ms	498	DCE	DTE	Frame Relay DLCI=100 InformationType=
11.7 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
4.9 ms	28	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=377 Timestamp=154
2.4 ms	498	DCE	DTE	Frame Relay DLCI=100 InformationType=
11.9 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
4.7 ms	28	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=378 Timestamp=154
1.6 ms	498	DCE	DTE	Frame Relay DLCI=100 InformationType=
9.9 ms	157	192.168.0.6	192.168.0.10	H.225 0 CONNECTION ID=Establish Capability
2.6 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
5.4 ms	28	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=379 Timestamp=154
1.1 ms	498	DCE	DTE	Frame Relay DLCI=100 InformationType=
13.8 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
2.5 ms	28	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=380 Timestamp=154
10.1 ms	498	DCE	DTE	Frame Relay DLCI=100 InformationType=
1.1 ms	28	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=5612 Timestamp=21
10.6 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
5.9 ms	28	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=381 Timestamp=154
380 ms	498	DCE	DTE	Frame Relay DLCI=100 InformationType=
1.1 ms	28	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=5613 Timestamp=21
11.6 ms	28	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
2.0 ms	28	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=382 Timestamp=154
1.1 ms	498	DCE	DTE	Frame Relay DLCI=100 InformationType=
1.1 ms	28	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=5614 Timestamp=21
10.2 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
6.3 ms	498	DCE	DTE	Frame Relay DLCI=100 InformationType=
1.1 ms	28	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=5615 Timestamp=21
1.5 ms	28	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=383 Timestamp=154
10.1 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S=X Windows Len=1
2.9 ms	28	192.168.0.6	192.168.0.10	RTP G.729 Audio Seq=384 Timestamp=154

Figura 30 - Medição Com QoS e Com LFI_540_G729 e Com rRTP

O tamanho do *payload* que antes era de 66bytes sem compressão, passou para 28 bytes comprimidos. Percebe-se, igualmente, que os valores de jitter tanto para aplicações *ftp* e voz são baixos. Garante-se que os testes foram bem sucedidos.

A garantia de que os testes foram bem sucedidos tem como suporte a intercalação dos pacotes, compressão de cabeçalho RTP, apenas um tráfego FTP de 1000bytes fragmentados em dois fragmentos de 548bytes e 498bytes.

A soma desses dois tráfegos não excede a capacidade total do link de acesso de 512kbps, embora tenha ficado tecnicamente no limiar. O maior valor do jitter foi de 5,9ms, ou seja, os fluxos fluíram muito bem durante os 120sec de conversas entre os ramais 4000 a 6000.

A fim de analisar os demais codecs, nas Figuras 31 e Figura 32, foi usado o codec G726 com compressão de cabeçalho, passando assim o payload de 126bytes para 88bytes comprimidos conforme a Figura 31 a seguir representa.

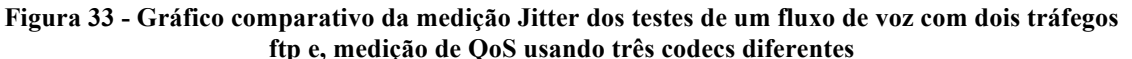
DeltaTime	Size	Destination	Source	Interpretation
9.6 ms	88	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37
12.1 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
6.3 ms	498	DCE	DTE	RTSP G.726 Audio Seq=37
3.9 ms	168	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37
3.9 ms	168	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
5.9 ms	168	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37
11.0 ms	498	DCE	DTE	RTSP G.726 Audio Seq=37
6.3 ms	498	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
292 us	168	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37
12.2 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
3.9 ms	168	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37
2.4 ms	498	DCE	DTE	RTSP G.726 Audio Seq=37
12.7 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
4.4 ms	168	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37
1.9 ms	498	DCE	DTE	RTSP G.726 Audio Seq=37
12.7 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
4.4 ms	168	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37
4.9 ms	168	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
13.9 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
3.9 ms	168	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37
1.6 ms	498	DCE	DTE	RTSP G.726 Audio Seq=37
3.6 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
3.9 ms	168	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37
4.9 ms	168	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
12.8 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
5.5 ms	168	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37
3.9 ms	168	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37
400 us	498	DCE	DTE	RTSP G.726 Audio Seq=37
12.6 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
5.9 ms	168	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37
1.1 ms	168	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37
12.6 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
6.0 ms	168	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37
4.9 ms	498	DCE	DTE	RTSP G.726 Audio Seq=37
3.9 ms	168	192.168.0.10	192.168.0.6	RTP G.726 Audio Seq=37
10.2 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
6.3 ms	498	DCE	DTE	RTSP G.726 Audio Seq=37
1.1 ms	168	192.168.0.10	192.168.0.6	RTP G.726 Audio Seq=37
3.9 ms	168	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37
12.1 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
5.0 ms	88	192.168.0.6	192.168.0.10	RTP G.726 Audio Seq=37

Figura 31 - Medição Com QoS e Com LFI_540_G726 e Com cRTP

Foram registradas algumas discrepâncias em termos de variação de atraso, algo que não aceita, quando comparado ao mesmo teste realizado com o codec G729. As demais características são semelhantes ao teste anterior, contudo, nesta situação, o *jitter* mais alto foi de 9,6sec para um dos fluxos de voz. Esse valor de jitter para este tipo de codec é, ainda, considerado mínimo, ou seja, abaixo do recomendado. Outrossim, pode-se perceber durante as conversações telefônicas entre os ramais que as ligações foram aceites, ou seja, foram boas. Na sequência desses testes, analisa-se a última ilustração - Figura 32 em que foram realizadas as medições usando o codec G711.

DeltaTime	Size	Destination	Source	Interpretation
9.6 ms	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37
3.9 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
6.3 ms	498	DCE	DTE	RTSP G.711 Audio Seq=37
3.9 ms	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37
3.9 ms	168	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
5.9 ms	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37
11.0 ms	498	DCE	DTE	RTSP G.711 Audio Seq=37
6.3 ms	498	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
292 us	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37
12.2 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
3.9 ms	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37
2.4 ms	498	DCE	DTE	RTSP G.711 Audio Seq=37
12.7 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
4.4 ms	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37
1.9 ms	498	DCE	DTE	RTSP G.711 Audio Seq=37
12.7 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
4.4 ms	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37
4.9 ms	168	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
13.9 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
3.9 ms	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37
1.6 ms	498	DCE	DTE	RTSP G.711 Audio Seq=37
3.6 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
3.9 ms	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37
4.9 ms	168	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
12.8 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
5.5 ms	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37
3.9 ms	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37
400 us	498	DCE	DTE	RTSP G.711 Audio Seq=37
12.6 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
5.9 ms	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37
1.1 ms	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37
12.6 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
6.0 ms	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37
4.9 ms	498	DCE	DTE	RTSP G.711 Audio Seq=37
3.9 ms	168	192.168.0.10	192.168.0.6	RTP G.711 Audio Seq=37
10.2 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
6.3 ms	498	DCE	DTE	RTSP G.711 Audio Seq=37
1.1 ms	168	192.168.0.10	192.168.0.6	RTP G.711 Audio Seq=37
3.9 ms	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37
12.1 ms	548	10.30.0.2	10.20.0.2	UDP D-COMPLEX LINK S
9.9 ms	168	192.168.0.6	192.168.0.10	RTP G.711 Audio Seq=37

Figura 32 - Medição Com QoS e Com LFI_540_G711 e Com cRTP



rede, ou seja, os tráfegos gerados pelos três codecs mais o tráfego de voz. Nesta ultima coluna, percebe-se de alguns altos picos, muito acima do limiar recomendado par aplicações de tempo real. Esses picos chegam a 99,10ms, pois são referentes aos fluxos de aplicações de dados.

Conclui-se que, sem a implementação de boa política de *QoS*, implementada para cada fila das três classes de serviços (CoS), os resultados seriam, de forma negativa, diferentes conforme demonstrados nas situações anteriores onde não houve qualquer tipo de manipulação de *QoS*, menos a fragmentação e compressão de cabeçalho. Com este gráfico, fecha-se esse capítulo, passando, deste modo, ao Capítulo VII - que trata dos resultados conclusivos de todas as medições, ou seja, permite abordar em síntese os resultados observados e inferidos a partir dos testes realizados, baseados no objetivo desta dissertação.

7 - CAPÍTULO VII – RESULTADOS COMPLEMENTARES - TESTES E MEDIÇÕES

“Nada há nada de mais poderoso do que uma idéia que chegou no tempo certo.”

– Vitor Hugo

“É triste falhar na vida; porém, mais triste é não tentar vencer.”

- Roosevelt

Neste capítulo VII, são descritos, em síntese, os resultados obtidos. É, também detalhado de forma objetiva o conjunto de procedimentos adotados para assim chegar a esses resultados e fechar, de forma conclusiva, esta dissertação, apresentando um conjunto de resultados que são evidenciados em uma matriz de valores.

7.1 - Resultados Finais

É apresentada a análise da matriz de resultados; a análise dos protocolos no domínio IP/MPLS e é apresentada uma seção de recomendações de boas práticas, e, na sequência, o Capítulo-VIII trata da conclusão da dissertação e sugestão futuros.

7.1.1 Matriz de resultados

A matriz (Tabela 24) a seguir representa uma matriz de valores observados a partir das medições e testes realizados, onde estão relacionados parâmetros como:

- ✓ Banda ocupada - economia de banda por aplicação e percentagem de otimização de banda;
- ✓ Tamanho de cabeçalho e, Jitter máximo por fluxos de voz;
- ✓ Tempo dedicados a cada sessão de testes;
- ✓ Quantidade de tráfego de voz e quantidade de tráfego do tipo FTP;

Taxa de pacotes por segundo; percentagem de perda; quantidade de *bytes* dos pacotes, de acordo com o codec utilizado; quantidade de canais de voz a ser adicionada quando ocorrer a compressão de cabeçalho, entre outros parâmetros, relacionado com três principais parâmetros a seguir:

- ✓ Compressão RTP / ou não compressão RTP;
- ✓ Utilização de pelo menos três codecs (G729, G726, e G711);
- ✓ Implementar políticas de QoS ou não implementar QoS;

Finalmente a habilitação do *link* de fragmentação e intercalação (LFI) ou não habilitação da LFI na interface FRF12. Uma vez elaborada essa matriz de valores, poder-se-á inferir os resultados seguintes, conforme se pode constatar na matriz Tabela 24 a seguir:

Tabela 24- Matriz dos Resultados de medidas de OoS, RTP e LFI usando os codecs G711/G726/G729

Inicialmente são realizados testes de compressão de cabeçalho RTP, a fim de avaliar a disponibilidade de banda de acordo com o codec usado. Desta forma, conforme a Tabela 24 pode ser percebido na primeira, segunda e terceira linhas os valores a seguir discriminados:

1. Na terceira linha (III) usando o codec G729, com reprodução de pacotes a 50pps, em uma conversa telefônica usando os ramis telefônicos R3000 a R6000, durante 8min com um jitter máximo de 25,8ms, usando apenas um canal de tráfego de voz (sem tráfego de dados FTP), com QoS habilitado, entretanto, sem compressão habilitada no acesso Frame Relay, foi observado que: - Dos 512kbps de banda disponível, foi ocupada 26kbps, o que equivale a 5,08% da banda total, dos 66bytes de pacotes *full* gerados por cada fluxo de sessão RTP, 46bytes são simplesmente cabeçalhos gerados pelos protocolos RTP e os das camadas anteriores (20-IP,8-UDP e 12-RTP e 6-Frame Relay, totalizando 46bytes de *overhead*), esse valor de *overhead* representa 69,69% de conteúdo não útil na rede que não teve perda de pacotes; Então, sem a compressão deve ser reservado no mínimo 26kbps de banda para apenas um (1) canal de voz. Se, no entanto, for reservada uma banda mínima de 60kbps para Classe de Serviço de tráfegos *real time* capacidade esta (60kbps) reservada segundo as políticas de provisão de garantia de QoS adotada pela rede da operadora para codecs de voz G729, essa banda reservada superaria a recomendação do próprio fabricante cisco [3][5], que recomenda reservar 11,60kbps em um enlace frame relay com cRTP incluindo já esse valor já um acréscimo de aproximadamente 30% sobre a banda a ser reservada para aplicações de tempo real e a cisco recomenda que seja reservado do mesmo jeito 26.8kbps de banda para quando não houver compressão RTP e 31,2kbps de banda reservada para enlace ethernet.

A OP adota uma reserva de 60kbps e codec G729 (sempre como perfil de tráfego na sua rede para aplicação voz). Sendo assim, para esse caso da ocupação de 26kbps por um canal de voz, ter-se-ia, mesmo assim, a banda economizada em 56,67% sendo que a banda ocupada foi de 43,33% caso a banda reservada fosse de 60kbps. Contudo, em um enlace de 512kbps a banda

foi otimizada em 94,92% e seria otimizada em 56,67% se fosse ocupada 60kbps para apenas um canal de voz considerando a banda total de 512kbps. Poderiam ser tratados 19 canais de voz sem compressão de cabeçalho (em uma banda total de 512kbps) o que equivale a ocupação da banda na ordem de 494kbps e sobrar-se-ia 18kbps de banda. Desses 18kbps, daria para tratar pelo menos mais um canal de voz comprimido e sobraria 8kbps de banda. Se, portanto, fosse tomado como referência de reserva da banda 60kbps, daria para colocar 2 canais de tráfego de voz não comprimida em paralelo, ou seja, adicionar-se-ia 2 (dois) canais de voz sem compressão que equivalem a 52kbps de ocupação já que sem a compressão um canal de voz ocupa 26kbps de banda e sobraria 8kbps a banda. Contudo se for tomado como referencia a banda total, seriam adicionados mais 18 canais de voz não comprimidos além do primeiro canal que ocupou 26kbps e mais 48 canais de voz comprimidos caso os equipamentos suportassem 48 canais.

2. Já de forma análoga a descrição acima centrada no item (1) na primeira linha (I) da matriz um tráfego de voz onde não houve perda de pacotes, entretanto com um jitter máximo de 20,2ms verificado em apenas um dos cinquenta (50) fluxos gerados em um segundo. Durante um tráfego de 8min, percebeu-se que devido a compressão de cabeçalho RTP, a banda ocupada foi de 10kbps, o que já representa uma vantagem de economia da banda de 38,46% em relação ao mesmo tráfego sem compressão de cabeçalho. Esses 10kbps representam ainda um total de 1,96% da banda total da rede. O cabeçalho do pacote *full* passou de um total de 66bytes para 28byte, o que implica dizer que cada fluxo comporta apenas 14,28% de cabeçalho, ou seja, essa rede trafega mais informação útil do que *overhead*.

Constata-se, ainda, que com a compressão apenas da banda de 26kbps, que antes fora utilizada por um único canal de voz, passará a comportar 2,6 canais de voz em paralelo, ou seja, podem ser colocados 2 (dois) canais de voz em paralelo e sobraria ainda 6kbps de banda. Ainda, se for tomado como banda reservada 60kbps e 512kbps com compressão seria suficiente para adicionar 6 canais e

51,2 canais, respectivamente. Uma diferença na ordem de 2 (dois) por 1 (um) em relação a um tráfego cujos fluxos não sofreram compressão RTP.

3. Na segunda linha (II), em condições semelhantes aos dois itens anteriores são gerados dois tráfegos de real time, através de conversação telefônica entre quatro pessoas, usando os seguintes ramais telefônicos do CPE02 (192.168.0.6) ramal 3000 para o CPE03 (192.168.0.10) ramal 5000 e, ligação telefônica do CPE02 (192.168.0.6) ramal 4000 para o CPE03 (192.168.0.10) ramal 6000. Este teste foi realizado com compressão habilitada, usando o codec G729 e dois canais de tráfegos de voz real time e inferiu-se que, o tamanho de bytes do quadro foi de 28bytes, não teve perda de quadros e a banda ocupada pelos dois canais foi de 20,6kbps o que equivale a 4,024% da banda total de 512kbps. O valor de 20,6kbps se refere ao resultado de estatística coletado na interface serial do roteador nos últimos 30s. O cisco permite fazer essa análise desabilitando o VAD, permitindo assim que o pacote seja reproduzido a taxa de 50pps. Ainda, com dois fluxos concorrentes, provou-se que a banda a ser economizada seria superior a apenas um fluxo de voz sem a compressão. Constatou-se que a banda fora economizada em 79,24% em relação a 43,33% que seria economizada em apenas um canal de voz sem a compressão de cabeçalho. Desta forma, não se pode concluir, com certeza absoluta, que um canal de voz comprimido ocupa justamente 10kbps, podendo assim, haver variações de alguns décimos de acréscimos, se não para este tráfego com dois canais de daria 20kbps ao invés de 20,6kbps. Entretanto, 10kbps é usado como referência nesta dissertação. Se utilizar o roteador Cisco discutido anteriormente como referência seria 11,6kbps.

Percebe-se ainda que usando esses parâmetros, a banda foi otimizada em 20,77% em relação a apenas um canal de voz que usou 26kbps e 95,98% em relação a capacidade máxima da rede e ainda foi constatado que caso fosse necessário adicionar mais canais de voz, que isso seria possível adiciona aos canais comprimidos existentes mais 18,90 canais sem a compressão, ou seja, a rede teria 2 (dois) canais de voz comprimidos e 18 canais de voz não comprimidos o que daria para somar 2 (dois) de 20 canais de voz e ainda

sobraria 9kbps de banda. Se, portanto, fosse necessário adicionar mais canais de voz, seria possível, por outro lado, adicionar além dos 2 (dois) canais de voz comprimidos, mais 23 (vinte e três) canais de voz comprimidos, totalizando 2 (dois) pares de 25 canais de voz comprimidos e sobriam ainda 8,5kbps de banda do total de enlace de 512kbps.

4. Na linha XVI, foi testada compressão de cabeçalho com G729 e com QoS/LFI habilitado, onde dois tráfegos FTP com taxa de reprodução de 30pps, foram colocados em paralelos com um fluxo de voz em tempo real. Chegou-se à conclusão de que não houve economia de banda, o que dificultou a possibilidade de otimização de banda, já que para os 400kbps reservados para tráfegos FTP mais os 60kbps reservado para tráfego de voz, totalizando 460kbps disponíveis, foi estimada uma estatística de ocupação de banda na ordem de 506,1kbps, capacidade quase no limiar da capacidade máxima da rede, ou seja, a banda reservada para classe *default* de 52kbps será realocada para essas três aplicações em caso de déficit da banda. O frame de voz como foi comprimido o RTP, cada fluxo de voz carregou um *overhead* de 14,28% e a rede sofreu uma perda de 2,15% sendo o *jitter* máximo para os fluxos de voz foi de 22,4ms. É de salientar, contudo, que a aplicação de tempo real tornou-se inviável o tempo todo devido aos elevados sequências de *jitter*.
5. Na linha XV, à semelhança do que aconteceu no item anterior, não houve compressão RTP, e não houve LFI habilitado na interface. Por conta deste último, é provável que a aplicação de tempo real seja prejudicada. As bandas reservadas para os dois tráfegos - um FTP e outro voz - ocuparam 449,6kbps dos 400kbps e 60kbps então reservados para CoS *business* (FTP) e voz, respectivamente. A banda foi, contudo, economizada em 62,4kbps dos 512kbps disponíveis na rede. Houve uma perda de 58% de pacotes, o *jitter* registrado para os fluxos de voz foi de 96,5ms, valor essa, em média, 5 vezes superior ao recomendado que é de 20ms.

Visto que os frames de voz não foram comprimidos, o tamanho de cabeçalho para cada fluxo RTP foi de 69,69%, ou seja, a rede carregou mais informação inútil do que útil para cada fluxo de voz que nela trafegou. A banda seria então,

nessas condições, otimizada em 10,4kbps do seu total de 512kbps o que é insignificante. Da banda economizada, daria para adicionar mais 2 canais de voz não comprimidos com a sobra de 4kbps dos 460kbps reservados e daria para adicionar mais 6 canais de voz comprimidas com a sobra de 2,4kbps de banda reservada. Essa prática revelou ser extremamente ineficaz e ineficiente. Seria assim, impossível, entender a conversação telefônica.

6. Na linha XIII, teste com compressão, QoS e LFI habilitados, usando o codec G729, a 50pps, durante 2min, o frame de voz *full de 66bytes*, com 69,69% de *overhead* para cada fluxo de voz, foi ocupado 403,6kbps de banda dos 460kbps reservados para as duas aplicações. Com essas configurações, foi registrada uma economia de 108,4kbps de banda do total de 512kbps e uma otimização de 56,40kbps para a banda reservada de 460kbps. Não foi, assim, necessário alocar recursos de banda disponível para a classe *default*. Dessa forma, aproveitando a otimização da banda, daria para acrescentar nesses 56,40kbps, mais 4 canais de voz não comprimidos e sobrariam 1,7kbps de banda e daria para adicionar mais 10 canais de voz comprimidos com restantes 8,4kbps de banda. O jitter máximo registrado foi de 5,9ms. Apesar da não compressão, o fluxo de voz não foi prejudicado pela intercalação de pacotes e a habilitação de políticas de QoS colaborou. Este não é uma caso ótimo, porém recomendado.
7. O teste resumido na linha XII da matriz, como diferença básica a habilitação de compressão provendo assim, ao contrário dos testes da linha XIII em que não houve a compressão RTP, a ocupação de banda em 390,6 kbps dos 460kbps, com uma otimização de banda reservada na ordem de 69,4kbps e uma banda total economizada em 121,4kbps, redução do cabeçalho e bytes full para 14,28% e 28bytes, respectivamente. Para essas aplicações não foi verificado qualquer perda de pacote, o jitter Máximo registrado foi de 5,9ms e conclui-se que da banda reservada a fatia economizada daria para adicionar 4,7 canais de voz não comprimidos, ou seja, 4 canais de voz não comprimidos e restantes 7kbps de banda e isso daria para adicionar além do canal de voz existente, mais 12,15 canais de voz comprimidos. Comparando o item XII e XIII, percebe-se que este caso é mais recomendado em comparação com o item XIII, pois este

-
- inclui a compressão de cabeçalho que resultou em vantagem expressiva, conforme acabado de ser exposto.
8. Já na linha VIII, foi usado o codec G726 com reprodução a 50pps durante dois minutos, com QoS/LFI e compressão de cabeçalho habilitado, o tamanho de bytes full passou de 126bytes para 88bytes. Desses 88bytes, 4bytes que equivalem a 4,55% são valores de *overhead*. A banda reservada foi de 400kbps para FTP e 51kbps para voz, totalizando 451kbps reservada para as duas aplicações do total de 512kbps total da rede; foi usada assim 400,3kbps de banda nas duas aplicações. Desse modo foi verificada uma economia de 111,7kbps da banda total e uma otimização de 50,7kbps da banda total reservada. O valor máximo de jitter registrado em um dos fluxos de voz foi de 9,6kbps e 0% de perda; foi também verificado que da banda economizada seria possível acrescentar mais 4 canais de voz não comprimidos e mais 11 canais de voz comprimidos.
 9. A linha IX mostra um caso análogo à linha VIII. A diferença é que não foi comprimido o cabeçalho RTP, logo, não foi registrado o tamanho da ocupação da banda. Entretanto, os quadros *full* foram de 126bytes que representou um overhead de 36,50% em cada fluxo de voz, ou seja, mais de 1/3 de informação são conteúdos inúteis. O jitter Máximo registrado foi de 20ms.
 10. À semelhança do item 9, a linha XI, foi testado o codec G726 sem compressão e QoS/LFI habilitado, foi verificado que, além do tráfego de tempo real carregar em cada fluxo um overhead de 36,50%, a rede comportou perda de informação na ordem de 2,30% e registrado jitter nos fluxos de voz na ordem de 96,5ms, embora o teste tenha sido de 8 minutos, isto é, 6 minutos a mais do que o teste do item 9.
 11. Na linha IV, é exibido o resultado de teste em que são testados compressão de cabeçalho, codec G711, habilitação de QoS e LFI e um tráfego que comporta duas classes de serviço - um FTP e outro voz - sendo ambas com taxa de reprodução de 50pps durante 120sec, percebeu-se que não houve perda de informação e que o jitter máximo foi de 9,9ms. Para a utilização do codec G711 o Cisco recomenda reservar para classe de voz banda na ordem de 83kbps.

Dessa forma, foi reservada 483kbps para os dois tráfegos concorrentes, 400kbps para dados e 83kbps para voz respectivamente. Entretanto, foi registrado a ocupação de banda na ordem de 407,8kbps, uma economia de 104,2kbps de banda total de 512kbps e uma otimização de banda na ordem de 75,2kbps do total de 483kbps reservado.

Dessa economia da banda, é possível acrescentar mais 4 canais de voz sem a compressão e mais 10 canais de voz comprimidos. Foi também registrado a diminuição do tamanho de bytes *full* de 206bytes para 168bytes, diminuindo, também, o conteúdo inútil carregado por cada fluxo RTP em 2,38%.

12. Já na linha V, seguindo as mesmas características e tráfegos descritos no item 11 acima, não foi registrado o tamanho de ocupação da banda, daí não ser possível inferir o tamanho da banda consumida e da banda otimizada, entretanto, como foi um teste sem compressão de cabeçalho, foi percebido, comparativamente ao sucedidos no item 11 anteriormente citado, que o tamanho de bytes *full* de quadro aumentou para 206bytes o que significa dizer que a rede transportou um overhead de 22,33% em cada 50 fluxo de voz – RTP, reproduzidos por segundos. Percebeu-se ainda que o jitter Máximo foi de 17,9ms.

13. Na linha VII, também à semelhança do item 12, não houve compressão de cabeçalho e não se verificou QoS habilitada e nem a fragmentação com intercalação habilitada, tendo sido registrado o jitter máximo de 50,8ms e com perda de 1,90% e *overhead* de 22,33%.

7.1.2 - Análise a nível do domínio backbone IP/MPLS

Na sequência dessas análises, é verificado o tamanho de frame, cabeçalho, payload, dados úteis e tipos de cada protocolo usado nos testes a partir de uma análise feita na interface serial do domínio do backbone MPLS.

A matriz da Tabela 25 a seguir representa os dados analisados em um teste, usando dois pares de ramais telefônicos com ligação em paralelo, partindo de CPE02 (192.168.0.6) ramal 3000 para o CPE03 (192.168.0.10) ramal 5000 e, ligação partindo do CPE02 (192.168.0.6) ramal 4000 para o CPE03 (192.168.0.10) ramal 6000.

Para essa análise foi usado o codec G729, analisando as informações a partir de telas capturadas no backbone IP/MPLS

	TIPO DE PROTOCOLOS	TAMANHO DO FRAME (Bytes)	CABEÇALHO (Bytes)	PAYLOAD (Bytes)	OVERHEAD (%)	DADOS UTIL	CODEC USADO
BACKBONE	FRAME FULL	78	58	20	74,35%	25,64%	G729
	ETHERNET	14					
	MPLS	4					
	IP	20					
	UDP	8					
	RTP	12					
	PAYLOAD	20					
ETHERNET	FRAME FULL	64	44	20	68,65%	31,25%	G729
	MPLS	4					
	IP	20					
	UDP	8					
	RTP	12					
	PAYLOAD	20					
MPLS	FRAME FULL	74	54	20	72,97%	27,02%	G729
	ETHERNET	14					
	IP	20					
	UDP	8					
	RTP	12					
	PAYLOAD	20					
	23 LABEL						
	5 EXP BIT						
	1 LABEL STACK						
	251 TTL						
IP	PACOTE FULL	60	40	20	66,66%	33,33%	G729
	IP	20					
	UDP	8					
	RTP	12					
	PAYLOAD	20					
UDP	DATAGRAMA F	40	20	20	50%	50%	G729
	UDP	8					
	RTP	12					
	PAYLOAD	20					
RTP	FRAME FULL	32	12	20	37,50%	62,50%	G729
	RTP	12					
	PAYLOAD	20					

Tabela 25 - Análise a partir do Backbone MPLS

A partir da interface do backbone MPLS, são analisados os seguintes itens: - Tipo de protocolo usado em cada camada, as informações de cabeçalho de cada protocolo.

- ✓ Por exemplo, considerando o protocolo MPLS, nota-se que foi identificado através dos números o label, bit EXP, *Label Stack*, número de TTL, além das informações do *frame full* de 74 bytes divididos da seguinte forma: em informações de payload e cabeçalhos, dessa forma em conteúdos de Cabeçalho sem compressão, pois em domínio de backbone não há compressão de cabeçalho, dessa forma obtém-se: 14bytes – quadros Ethernet; 20bytes para pacotes IP, 8bytes UDP, 12bytes de RTP e finalmente 20bytes de conteúdo útil (*payload*). Conclui-se que usando o codec G729, as informações no domínio MPLS dos 74bytes *full*, 54bytes são *overhead* o que representa 20 bytes *payload*, traduzindo-se em 72,92% e 27,02% de *overhead* e dados úteis, respectivamente.

- ✓ No domínio do backbone MPLS, são contudo, exibidas todas as informações dos protocolos usados, como: Ethernet, MPLS, IP, UDP, RTP e a informação do conteúdo de dados úteis – *payload*. No domínio MPLS é carregado, todavia, a maior quantidade de *overhead* se comparado com os demais da tabela. Do *frame full* de 78bytes, 58bytes representam informação de cabeçalho que equivale a 74,35% de informação inútil e os restantes são 25,64% de dados úteis que são 20bytes de *payload*.
- ✓ No domínio Ethernet, o frame é de 64bytes, sendo 44bytes equivalentes a 68,65% de overhead e 20bytes que correspondem a 31,23% de dados úteis. Nessa análise são, também, exibidas as informações sobre o protocolo, embora tal como exibidas as informações do protocolo MPLS, embora, nesta tabela tenham sido ilustradas apenas as informações para o protocolo MPLS, pois, na seção que trata de compressão RTP, essas informações são mostradas em tabelas próprias.
- ✓ No nível IP, o pacote *completo* é de 60bytes, 40bytes equivalentes a 66,33% de *overhead* e 20bytes equivalentes a 33,33% de dados úteis, ou seja, sem a compressão o pacote IP transporta mais overhead do que dados úteis.
- ✓ No domínio UDP, o datagrama é de 40 bytes, 20bytes para *payload* e 20bytes para *overhead*, ou seja, 50% para dados úteis e 50% para *overhead*, usando o codec G729.
- ✓ A nível do protocolo RTP, do total de 32bytes, 20 bytes são *payload* 12bytes overhead, o que significa que 37,50% são *overhead* e 62,50% são dados úteis.

A seguir são ilustradas algumas tabelas que representam a síntese dos resultados expostos acima, de acordo com a matriz da Tabela 24.

7.1.3 - Síntese dos resultados

As tabelas a seguir representam a síntese dos resultados em uma visão simplificada da matriz da Tabela 24, conforme seguem: A Tabela 26 representa os ganhos em termos de quantidades de canais VoIP a ser adicionado usando codec G729,

com LFI e QoS habilitados em um tráfego inicial com apenas um canal de voz e dois tráfegos FTP, concluindo que

QoS(LFI 540bytes), G729, cRTP: 2*FTP +1 *Voz							
BANDA Total(kbps)	BANDA Ocupada(kbps)	Jitter Max (ms)	Canais add. RTP	Canais add. cRTP	Total Canal Voz RTP	Total Canal Voz cRTP	Perda de pacotes (%)
512	506,1	22,4	0	1	0	1	2.15%

Tabela 26 - Quantidades de canais VoIP usando G729 com LFI e cRTP

em termos de ganhos, de acordo com a Tabela 26, a banda foi estourada apesar da estatística da ocupação da banda dos últimos 30sec ser de 506.1kbps. Esse provável estouro da banda gerou perda de pacotes na ordem de 2,15%, não tendo sido possível acrescentar algum outro canal, ainda que fossem comprimidos os quadros de voz.

Considerando um caso semelhante, embora com dois canais de voz sem nenhum tráfego de dados em paralelo, conclui-se com base na Tabela 27 a seguir, que com a compressão de cabeçalho, o enlace suportaria mais dois pares de 23 canais de voz totalizando 46 canais de voz

QoS, G729, cRTP: 2*PARES DE CANAIS DE VOZ (Sem Dados FTP)							
BANDA Total(kbps)	BANDA Ocupada(kbps)	Jitter Max (ms)	Canais add. RTP	Canais add. cRTP	Total Canal Voz RTP	Total Canal Voz cRTP	Perda de pacotes (%)
512	~ 503,5	NR	2*9	2*23	18	48	0%

Tabela 27 - Quantidade de canais considerando QoS, LFI e cRTP habilitados sem dados

ao invés dos 18 canais sem a compressão de cabeçalho; o valor máximo de jitter não foi registrado (NR). Já realizando testes com políticas totalmente diferentes, onde não foi habilitado o LFI e cRTP, ou seja, sem quaisquer políticas de QoS, embora com codec G729 registrou-se o jitter máximo de 96,5, perda de 58% de dados FTP. Portanto, com a compressão

SEM QoS (nLFI 1000bytes) RTP,G729							
BANDA Total(kbps)	BANDA Ocupada(kbps)	Jiiter Max (ms)	Canais add. RTP	Canais add. cRTP	Total Canal Voz RTP	Total Canal Voz cRTP	Perda de pacotes (%)
512	449,6	96,5	2	6	3	7	58%

Tabela 28 - Quantidades de canais em tráfegos VoIP sem QoS e sem cRTP usando G729

RTP o número máximo de canais de voz possível de acrescentar são 7, ao invés de 3 canais sem cRTP, conforme a Tabela 28.

Considerando desta forma, a alternância do codec para G711, com compressão RTP (cRTP) habilitada, fragmento a 640bytes e com QoS, foram obtidos os mesmos valores de canais de voz a suportar quando for comprimido o cabeçalho, ou seja, 11 canais de voz comprimidos são suportadas; as mesmas quantidades de canais são também no máximo suportadas para os testes realizados usando codec G729, sem compressão RTP e fragmentos a 540bytes. As duas tabelas seguintes (Tabela 29 e Tabela 30) apresentam algumas diferenças, a saber:

QoS(LFI 640bytes), G711, cRTP							
BANDA Total(kbps)	BANDA Ocupada(kbps)	Jitter Max (ms)	Canais add. RTP	Canais add. cRTP	Total Canal Voz RTP	Total Canal Voz cRTP	Perda de pacotes (%)
512	407,8	9,9	4	10	5	11	0%

Tabela 29 - Quantidades de canais VoIP em enlace 512kbps, LFI-640bytes, G711 e cRTP

- Nas mesmas condições, o G711 apresenta maior valor de jitter do que o G729, relação de 9.9ms para 5.9ms respectivamente e o G711 ocupou maior capacidade de banda;

Com QoS, com LFI 640 G729 e sem cRTP							
BANDA Total(kbps)	BANDA Ocupada(kbps)	Jiiter Max (ms)	Canais add. RTP	Canais add. cRTP	Total Canal Voz RTP	Total Canal Voz cRTP	Perda de pacotes (%)
512	403,6	5,9	4	10	5	11	0%

Tabela 30 - Quantidades de canais VoIP em enlace 512kbps, LFI -540bytes, G729 sem cRTP

Nos testes anteriores, considerando as duas tabelas (Tabelas 29 e Tabela 30) não houve perda de pacotes. Um outro teste também realizado usando o G729 com fragmentação a 640bytes e com cRTP, conforme mostra a Tabela-31 a seguirTabela 31, é possível ter 13 canais de voz disputando meio

QoS(LFI 640bytes), G729, cRTP							
BANDA Total(kbps)	BANDA Ocupada(kbps)	Jitter Max (ms)	Canais add. RTP	Canais add. cRTP	Total Canal Voz RTP	Total Canal Voz cRTP	Perda de pacotes (%)
512	390,6	5,9	5	12	6	13	0%

Tabela 31 - Quantidades de canais VoIP em enlace 512kbps, LFI-640bytes, G729 e cRTP

com dados FTP, sem que haja perda de dados e a um jitter Máximo de 5,9ms, mesmo valor do jitter se comparado com os resultados da Tabela 31, já este com menor consumo da banda. Alternando, novamente, o tipo de codec de voz para o G726, com LFI a 640bytes e compressão RTP habilitado (Tabela 32Tabela 32) com um jitter de

9,6ms e 0% de perda, com cRTP poderá haver 12 canais de voz comprimidos disputando a banda com dados do tipo FTP em paralelo.

QoS(LFI 640bytes), G726, cRTP							
BANDA Total(kbps)	BANDA Ocupada(kbps)	Jitter Max (ms)	Canais add. RTP	Canais add. cRTP	Total Canal Voz RTP	Total Canal Voz cRTP	Perda de pacotes (%)
512	400,3	9,6	4	11	5	12	0%

Tabela 32 - Quantidades de canais VoIP em enlace 512kbps, LFI-640bytes, G726 e cRTP

Essa quantidade de 12 (doze) canais de voz é sem duvida três (3) vezes superior ao limite máximo de 4 (quatro) canais de voz, sem compressão de cabeçalho RTP, inicialmente suportados. São, inicialmente, realizados pelo menos dois testes de compressão, onde são aferidas a média da ocupação de banda nos últimos 30sec registrado na interface serial dos roteadores, o valor do *jitter* Máximo bem como a quantidade de canais de voz que são possíveis de existir em enlace de 512kbps. Nesse sentido as próximas duas tabelas (Tabela 33 e Tabela 34) retratam essas observações.

QoS, G729, RTP (Sem Dados FTP)							
BANDA Total(kbps)	BANDA Ocupada(kbps)	Jitter Max (ms)	Canais add. RTP	Canais add. cRTP	Total Canal Voz RTP	Total Canal Voz cRTP	Perda de pacotes (%)
512	~ 505,1	25,8	17	47	18	48	0%

Tabela 33 - Quantidade de canais de VoIP em enlace 512kbps sem cRTP, com QoS e G729

Analisando a Tabela 33, conclui-se que em link de 512kbps, com filas FIFO, conseguir-se-ia ter mais 48 canais de VoIP comprimidos, contra 18 canais de voz não comprimidos, com um jitter máximo de 25,8ms registrado em apenas um dos fluxos de voz, entre centenas de fluxos em um tráfego usando G729 e com QoS habilitado. Já no caso onde foi comprimido os frames de voz, habilitada a QoS com filas FIFO e compressão RTP, o jitter foi de 20,2ms, 0% de perda de frames, com 52 canais de voz comprimidos, conforme evidencia a Tabela-34 a seguir. Com a compressão seria possível colocar, neste caso, até 52 canais de voz, caso os equipamentos suportassem essa quantidade, pois os equipamentos testados suportam até o Máximo de 48 canais de voz [38],[40].

QoS, G729, cRTP (Sem Dados FTP)							
BANDA Total(kbps)	BANDA Ocupada(kbps)	Jitter Max (ms)	Canais add. RTP	Canais add. cRTP	Total Canal Voz RTP	Total Canal Voz cRTP	Perda de pacotes (%)
512	~ 504,0	20,2	19	51	20	52	0%

Tabela 34 - Quantidade de canais de VoIP em enlace 512kbps com cRTP, com QoS e G729

A ocupação da banda de acordo com a Tabela 34, são valores aproximados dos últimos 30sec. Entretanto, percebe-se assim, que caso os testes fossem inicialmente realizados com compressão de cabeçalho, conseguir-se-iam mais canais comprimidos do que menos canais de voz comprimidos posteriormente ao serem adicionados à banda otimizada dos testes iniciais sem a compressão de cabeçalho, ou seja, a cRTP deve, neste caso, ser habilitado sempre. Dos testes realizados concluiu-se que os valores de jitter são de um modo geral aceitáveis dentro do limite recomendado 20ms a 30ms; Percebeu-se que conforme as informações são transmitidas, ao serem recebidas, as do cabeçalho são retiradas de acordo com o nível de rede e dos protocolos usados. Sendo assim, o RTP, carrega mais informações úteis do que lixos de *overhead*. A seguir a matriz da Tabela 35 a seguir relaciona a ocupação de banda em termos percentuais por cada teste realizado.

7.1.4 – Matriz de percentual de ocupação da banda por cada teste

A fim de permitir uma comparação mais precisa a Tabela 35 a seguir mostra a ocupação da banda por pelo menos cinco diferentes tipos de testes realizados, levando em conta a banda total 512kbps.

Nun	Descrição de Testes	Banda ocupada (%)	Banda Total (kbps)
1	Banda ocupada na medição Sem QoS, Sem cRTP, sem LFI -640bytes, G729 (1 voz +1 FTP).	87,82%	512kbps
2	Ocupação da Banda nos testes Com QoS, com cRTP, com LFI-540bytes, G711 (1 voz +1 FTP).	79,65%	
3	Banda ocupada na medição com QoS, Sem cRTP, com LFI-640bytes, G729 (1 voz +1 FTP).	78,83%	
4	Ocupação da Banda nos testes Com QoS, com cRTP, com LFI-540bytes, G726 (1 voz +1 FTP).	78,19%	
5	Ocupação da Banda nos testes Com QoS, com cRTP, com LFI-540bytes, G729 (1 voz +1 FTP).	76,29%	
6	Ocupação da Banda nos testes Com QoS, com cRTP, com LFI-540bytes, G729 (1voz+2 FTP).	98,83%	

Tabela 35 - Matriz de percentual de ocupação da banda por cada teste

Na matriz da Tabela 35 conclui-se que a capacidade da banda ocupada por um tráfego envolvendo codec G729 com QoS, sem compressão de cabeçalho e LFI habilitado ocupa aproximadamente a mesma banda que um tráfego comportado pelo

codec G726, com compressão de cabeçalho e LFI habilitado, tomando como referência a banda total disponível. Todos os tráfegos comportando um fluxo de voz e um tráfego FTP, ambos os testes com as mesmas características.

Conclui-se, portanto, que o melhor resultado é do codec G729, com QoS, LFI e compressão RTP habilitados. Nas mesmas condições, esse passa a ser o pior dos casos, se colocado dois tráfegos FTP de 1000bytes cada a pelo menos 30pps e um canal de voz, conforme a tabela, o resultado de 98,83% seria o pior caso, apesar de todas as políticas de QoS terem sido implementadas. No entanto, não foram respeitados os limites do parâmetro CIR.

7.1.5 – Recomendações de boas práticas

Para se chegar a esses valores, um conjunto de procedimentos deve ser adotado, entre os quais cabe citar:

1. Preparar o laboratório de teste em termos de hardware e software, conforme o modelo da topologia lógica anteriormente exibida;
2. Ter auxílio de pelo menos mais três pessoas (total de 4) para realizar alguns testes com, *p.ex.*, quando se vai realizar testes de *real time* usando dois pares de ramais telefônicos;
3. Para enlace de baixa capacidade, como é o caso da banda disponível de 512kbps em estudo, onde esse canal compartilha dados do tipo FTP, com aplicações de tempo real como voz. Baseado nos resultados expostos anteriormente, algumas recomendações são aceitáveis conforme se pode ver nos itens que seguem:
 - 3.1 – Escolher o codec de voz a ser utilizado neste caso é recomendado o G729, pela sua melhor adequação em todos os testes;
 - 3.2 – Implementar políticas rígidas de QoS DiffServ, tipo de fila *Strict Priority* para CoS de voz e *Fair Queuing* para CoS FTP e FIFO para classe *default*;
 - 3.3 – Alocar a abanda para cada aplicação com uma folga de, no mínimo, 10% da banda;
 - 3.4 – Realizar sempre a compressão de cabeçalho RTP, a fim de otimizar a banda, possibilitando, assim, adicionar mais canais de voz, ao invés da rede comportar grande percentagem de overhead em cada fluxo de voz transportado;
 - 3.5 – Habilitar também a compressão IP/UDP a nível dos pacotes dos dados; deve também trazer maiores benefícios no quesito otimização da banda;
 - 3.6 – Habilitar sempre a fragmentação com intercalação de pacotes;

-
- 3.7 - Usar preferencialmente o Codec G729, pois este possui menor retardo de envio e formação de um quadro de voz na ordem de 10 a 15ms; permite a codificação de voz com em 8kbps; atraso máximo de codificação típico do algoritmo de 0.250ms. O sinal é amostrado a uma taxa de 8khz, assim, cada amostra é quantizada/quantificada com 8bits, a uma taxa de 8kbps, com o tempo necessário para formar um quadro em 10ms e quando aplicado a compressão de cabeçalho em enlace FRF.12 este tem a menor ocupação de banda na ordem de 11.6 Kbps, entre outras características que o diferem dos demais;
- 3.8 – Se considerado economia da banda como requisito os codecs devem ser usados na seguinte ordem de preferência: G729,G726 e o G711;
- 3.9 - Considerando a qualidade do sinal da voz como requisito deve, entretanto, ser usado o G711 como primeira preferência apesar de demandar muita banda e em segundo o G726.
- 3.10 – A prática recomenda que independentemente do codec deve ser combinado a técnica de compressão RTP com LFI de pacotes, quando a banda for considerada baixa.
- 3.11 - Recomenda-se, para casos como propõe o objetivo desta dissertação, usar a combinação de compressão RTP com G729 e com habilitação de QoS e LFI.
- 3.12 – O mesmo número de canais comportará um tráfego de voz usando a combinação das técnicas de compressão de cabeçalho (cRTP) + G711 e ou usando a combinação G729 sem compressão de cabeçalho, ou seja, o G729 apresenta um melhor algoritmo de compressão se comparado com o G711;
4. Seguindo esses critérios, chega-se a um conjunto de resultados satisfatórios apresentados na matriz (Tabela 24) dos resultados acima, que satisfaça em definitivo o estudo proposto, passando assim ao Capítulo VIII que trata da conclusão e trabalhos futuros da dissertação conforme seguem nas próximas paginas.

8 - CAPÍTULO VIII – CONCLUSÃO DA DISSERTAÇÃO E ESTUDOS FUTUROS

"A força não provém da capacidade física e sim de uma vontade indomável."
- **GANDHI**

"Quem não quer pensar é um fanático; quem não pode pensar é um cretino; quem não ousa pensar é um covarde."
- **Sir FRANCIS BACON**

8.1 - Conclusão técnica.

A Matriz da Tabela 36 a seguir representa o resumo afirmativo da conclusão para este estudo dissertativo, conforme se lê na Tabela 36. Esta matriz (Tabela 36) relaciona a quantidade máxima de canais VoIP que podem ser tratados em um canal de 512kbps de banda total compartilhada. Dessa banda, pelo menos 400kbps de banda é reservada para dados e apenas 60kbps é reservada para aplicação Voz em tempo real.

Aplicando as técnicas de melhoria de desempenho de enlace como: QoS DiffServ; LFI; cRTP; e uso de alguns Codecs como o G729, G726 e G711; e correlacionando essas técnicas usando o marcador "X", pode-se afirmar quais os números máximos de canais VoIP podem ser tratados, considerando a banda de apenas 60kbps reservados a voz, enquanto dados são paralelamente trafegados em um outra fila.

O marcador "X" em uma mesma linha, diz a quantidade máxima de canais possíveis de serem tratados se for implementado serviços VoIP levando em conta a habilitação em conjunto de cada uma das técnicas marcadas pelo "X". A Tabela 36 a seguir apresenta uma síntese.

Banda Voz (60kbps)						
Qtde Canais VoIP	QoS DiffServ	LFI	cRTP	G729	G726	G711
1		x		x	x	
1		x	x			x
2		x		x		
2	x	x	x		x	x
3	x	x	x	x		
4	x	x	x	x		
5	x	x	x	x		

Tabela 36 - Matriz Quantidade de canais banda disponível para VoIP

Da Tabela 36, conclui-se em relação a banda disponível para aplicação VoIP que:

-
- 1 – É Sempre necessário a aplicação de LFI para garantir a qualidade de sinal independente de quantidade de canais VoIP desde que existem dados compartilhando o canal;
 - 2 – Se houver (um) 1 canal VoIP a ser tratado, este funciona bem sem a QoS, e sem a cRTP, mas com alguns picos, usando o G729 /G726, já para o G711 precisa da cRTP;
 - 3 - Para tratar até (dois) 2 canais, usa G729 sem QoS e sem a compressão, funciona contudo com alguns picos de jitter. Fica inviabilizada a comunicação, se for usado o G711 e o G726, precisando contudo da habilitação da cRTP, LFI,QoS;
 - 4 – Se for tratado de 3 canais em diante, ate 5 canis VoIP, para a banda de 60kbps, garante-se VoIP de boa qualidade usando apenas o G729 associado a técnicas de QoS *DiffServ*, LFI,cRTP.
 - 5 – Se for usado o G711 sem cRTP não se pode ter um (1) único canal VoIP

8.2 - Conclusão do estudo dissertativo

Com base no objetivo preconizado pelo estudo e elaboração desta dissertação – conforme sugere o título - conclui-se que esta dissertação permitiu que fossem apresentados resultados traduzidos em soluções viáveis para a avaliação de serviços VoIP em redes de baixa velocidade, onde o link foi compartilhado para transmissão de dados em paralelo. Feito isso, chegou-se ao objetivo pretendido embora, ainda faltariam algumas medições a serem feitas;

As medições julgadas interessantes de serem feitas estão relacionadas a seguir como trabalhos futuros. Alguns testes complementares não foram realizados na época devido a indisponibilidade da operadora em continuar alocar laboratórios, técnicos, bem como equipamentos que permitissem realizar a interoperabilidade entre equipamentos de fabricantes diferentes; O FRF.12, atendeu de forma integral o objetivo - trabalhar com VoIP em enlace de baixa capacidade que trafega dados; Foi muito proveitoso a parceria com a operadora, uma vez que permitiu a prática laboratorial em um ambiente peculiarmente técnico;

Ademais, com este trabalho, percebeu-se que ainda, é possível oferecer bons serviços VoIP em links de baixa capacidade, ou seja ainda operadora podem usar esse tipo de serviço para determinados clientes. Provou-se que quando se trata de enlace de baixa capacidade com tráfegos de dados compartilhado, é recomendado aplicar sempre técnicas de melhorias de desempenho ao enlace como cRTP, QoS devidamente implementada, escolha de codec, etc, para poder oferecer também Serviços VoIP. Usando os recursos laboratoriais, principalmente, do CRT- LOP e outros tantos do Laboratório da FIRJAN, no âmbito do acordo de cooperação técnica firmada entre esse Laboratório e a UFF, surge assim a oportunidade de investigar e solucionar um problema que na ocasião era tão pertinente para a OP como oportuno para a Universidade que tinha interesse em exercitar os alunos de forma prática. Foi assim que surgiu essa excelente oportunidade para desenvolver, de forma prática, este trabalho que conta, portanto, no estágio atual com um conjunto de resultados provenientes das medições realizadas durante mais de um semestre letivo.

Com a ajuda dos técnicos, foram montadas estruturas e criadas espaço e ambiente propícios para a realização dos testes para a operação da rede e na rede. Convém afirmar que os testes tiveram acompanhamento direto da OP que também acompanhou nos testes realizados na FIRJAN quando ela (OP) não dispunha de determinados equipamentos.

Foi, a partir, desses cenários onde se levou a cabo a execução das tarefas, que passou-se a escrever os resultados finais que se traduzem no seguinte: Uma matriz de resultados onde são abordados os aspectos considerados mais importantes nas medições; um “Caderno de recomendações das boas práticas laboratoriais”, para testes do gênero. Os resultados obtidos foram avaliados e comprovados, conforme se pode verificar na seção dos resultados parciais e conclusivos desta dissertação. A adequação dos codecs em relação aos equipamentos, sendo no nosso caso o G729, para plataformas Cisco revelou-se ser mais eficaz; a viabilidade de intercalação dos frames de voz entre os pacotes grandes do tipo FTP – procedimento, concluído, muito necessário, uma vez que a fragmentação tenha sido devidamente habilitada e cooperou de forma positiva. Outro importante fato registrado é a implementação de políticas de QoS rígidas, ou seja,

de acordo com a política de implementação de QoS em suas redes, as técnicas como compressão RTP, habilitação de *Link Fragmentation and Interleaving* (LFI), são “funções” intrínsecas ao planejamento e implementação das demais políticas de QoS.

Dessa forma, a implementação de QoS *DiffServ* permitiu de forma aconselhável que fossem criados três tipos básicos de Classe de Serviços, cujas bandas foram bem divididas e as aplicações devidamente marcadas. Foi um procedimento indispensável para que fosse possível chegar a estes resultados. A técnica de QoS foi raras vezes dispensável, pelo fato da banda ser estreita e compartilhada. Dito isso, conclui-se, também, que adotando essa política e todas essas técnicas em conjunto, tornar-se-ia possível projetar rede de serviço multimídia, a baixo custo e com serviços de qualidade. Todas essas técnicas em conjunto, permitem manter em funcionamento de forma eficaz e eficiente uma rede já considerada inadequada para os dias de hoje, desde que haja sempre uma boa política administrativa de modelagem de tráfego de forma conveniente.

Em termos práticos e comerciais, percebeu-se, também, que além da redução de ocupação da banda que antes comportava mais de 50% de conteúdo inútil, abriu-se espaço para alocar de forma eficiente o enlace, ou seja, ao invés de ter um ou dois canais de voz, em paralelo com links de dados, o mesmo link passou a comportar o dobro ou triplo de canais de voz, para uma banda estreita reservada para tráfegos de voz, na ordem decimal de 60kbps reservados.

Comprovou-se também de forma comparativa os resultados de atraso, jitter, a ocupação da banda, compressão, entre outros parâmetros de medidas de cada aplicação relacionando estes às normas padronizadas e recomendações.

Dentre essas medidas, percebe-se que *p.ex.* o codec G726 tem o menor consumo de banda do que o G711 apesar deles possuírem qualidades semelhantes, este embora, ainda muito usado em sistemas telefônicos e transmissão de voz que exige pouco processamento, vem perdendo espaço para o codec G.729, devido a sua incapacidade de trabalhar com bandas passantes baixas, quando comparado com o G.729.

Conclui-se ainda que o tempo necessário para se formar um quadro usando este codec é por *default* 30ms, enquanto que o G729 precisa de 10ms a 15ms, ou seja, o

G729 apresenta, neste aspecto, uma vantagem na ordem de 50%. Já com relação ao G711 é necessário um atraso mínimo de 20ms para formação de um quadro [35]. Esse codec, porém, ocupa mais banda em uma rede Ethernet ou FRF.12 do que quaisquer outros codecs, o que implica dizer que não é aconselhado para enlaces de baixa capacidade, o que implica em elevados jitter, apesar da sua boa qualidade de aderência ao fluxos de voz. Conclui-se que o link comporta o mesmo número de canais de voz combinando as técnicas de compressão de cabeçalho (cRTP) + G711, ou usando a combinação G729 sem cRTP.

Conclui-se que independentemente das políticas de QoS e modelagem de tráfego em Frame Relay aplicadas, ainda que haja banda disponível na rede, a não implementação da LFI inviabiliza toda a comunicação VoIP se a banda for compartilhada com dados.

Concluiu-se também que independentemente da taxa de reprodução e da banda disponível, o valor de delay (atraso) que os pacotes e ou os quadros toleram de acordo com o enlace onde são testados, com jitter a cima dos 20 ms recomendados, degradou a qualidade do sinal de forma grosseira entre os dois ramais. Verificou-se que a perda de pacotes ocorreu indiscriminadamente, quando não se teve o cuidado de gerenciar adequadamente a banda. Como principais contribuições, destacam-se a introdução eficaz do *software free* – MGEN no cenário do LOP, a Matriz de resultados e a seção de recomendações de boas práticas laboratoriais, conforme retratadas nas seções dos capítulos anteriores. O capítulo XII – apêndice, trás algumas telas complementares que facilitam o entendimento de alguns testes cujos resultados forma bem inferidos.

Por fim, algumas análises não chegaram a ser realizadas, por motivos relacionados com a indisponibilidade operacional do LOP (Laboratório de Operadora de Telecomunicações). Esses mesmos testes hoje julgados interessantes de serem realizados, estão relatados na seção – Estudos futuros, que caso houver oportunidade e interesse das entidades participantes, seria interessante desses testes complementares, ainda que seja para fins puramente instrutivos, já que os mesmos são de natureza prática, consolidando teoria à prática.

8.3 - Estudos futuros:

Uma vez encerradas as medições no pólo tecnológico da OP (Operadora de Telecomunicações), avançamos com a compilação dos relatórios. Foi nessa altura que se constatou que seria necessário a realização de alguns testes adicionais refutados de capital importância. Chegou-se a conclusão de que a realização de tais testes era interessante e que os mesmos serão contemplados como estudos futuros.

- ✓ Compressão de cabeçalho dos dados FTP além dos dados *Real time* a fim de avaliar a disponibilidade de banda, já que os pacotes de dados são maiores;
- ✓ Apesar de realizações dos testes: com QoS e com LFI ; seria também interessante realizar teste tipo: teste com QoS e sem LFI;
- ✓ Uma vez realizados os testes: sem QoS e sem LFI, seria interessante a realização dos testes sem QoS e com LFI;
- ✓ Testes em que os dois tráfegos (Voz e Dados) tivessem as mesmas prioridades (p.ex. Filas - Fair Queue) na fila e com intercalação de pacotes e, sem intercalação de pacotes.
- ✓ Teste com conversas telefônicas envolvendo, simultaneamente, quatro ou mais pessoas;
- ✓ Repetir os testes usando outros codecs de voz e outros equipamentos de comutação;
- ✓ Testes com compressão de cabeçalho habilitado e sem intercalação dos pacotes usando pelo menos três diferentes codecs: G711, G726, e G729;

Os próximos capítulos tratam de Referencias bibliográficas, Apêndice, e anexos conforme seguem na seguinte ordem os Capítulos: IX, X e XI, respectivamente.

9 - CAPÍTULO IX – REFERÊNCIAS BIBLIOGRÁFICAS & REFERÊNCIAS CONSULTADAS

“Ninguém é tão sábio que nada tenha para aprender, nem tão tolo que nada tenha pra ensinar”.
- BLAISE PASCAL

9.1 - REFERÊNCIAS BIBLIOGRÁFICAS

- [1] –Frame Relay Queueing and Fragmentation at the Interface. Disponível em: http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_frque_frag_if.html Acesso Junho /2007
- [2] - Andrew G. Malis, *Frame Relay Fragmentation Implementation Agreement - FRF.1*, disponível em: <http://www.broadband-forum.org/technical/download/FRF.12/frf12.pdf> Acesso em 11.2010
- [3] - Understanding Delay in Packet Voice Networks bandwidth Consume. Disponível em: http://www.cisco.com/warp/public/788/pkt-voicegeneral/bwidth_consume.pdf Acesso em 05.2007.
- [4] - VoFR Encapsulation and Fragmentation: Disponível em: http://www.cisco.com/warp/public/788/voip/vofr_encap_frag_5733.pdf Acessado em 11.2006.
- [5] - Voice over IP – Per Call Bandwidth Consumption. Disponível em: http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml Acesso em 05.2007
- [6] - *Understanding CODECs: Complexity, Hardware Support, MOS and Negotiation* . Disponível em: http://www.cisco.com/warp/public/788/voip/codec_complexity.html Acesso em 05.2007
- [7] - Resolve IP Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPSEC. Disponível em http://www.cisco.com/warp/public/105/pmtud_ipfrag.pdf Acesso em 04.2007
- [8] – Redes de Computadores e a Internet: uma nova abordagem - Kurose, James F. e Ross, Keith W, 1ª ed S. Paulo: Addilson Wesley, 2003...
- [9] - Frame Relay Fórum v12 – FRF.12 : Disponível em: <http://www.mfaforum.org/frame/Approved/FRF.12/frf12.pdf> Acessado em 11.2006
- [10] - VoIP over Frame Relay with Quality of Service (Fragmentation, Traffic Shaping, LLQ / IP RTP Priority) – Disponível em: <http://www.cisco.com/warp/public/788/voice-qos/voip-ov-fr-qos.pdf> : acesso em 11.2006

-
- [11] - Understanding Delay in Packet Voice Networks Disponível em : <http://www.cisco.com/warp/public/788/voip/delay-details.pdf> acesso em 11.2006
- [12] – FRF.12 Policing and Shaping Overview, Disponível em http://www.cisco.com/en/US/docs/ios/12_0/qos/configuration/guide/qcpolts.html Acesso em 03.2007.
- [13] - Token Bucket Concept Used in CAR. Disponível em: <http://book.soundonair.ru/cisco/ch23lev1sec1.html> acessado em 03.2007.
- [14] - VoIP over Frame Relay with Quality of Service (Fragmentation, Traffic Shaping, LLQ / IP RTP Priority). Disponível em: <http://www.cisco.com/warp/public/788/voice-qos/voip-ov-fr-qos.pdf> Acesso Junho /2007
- [15] - VoIP over PPP Links with Quality of Service (LLQ / IP RTP Priority, LFI, cRTP) Disponível em : <http://www.cisco.com/warp/public/788/voice-qos/voip-mlppp.pdf> Acessado em 03.2007.
- [16] - Frame Relay Fragmentation Implementation Agreement FRF.12. Disponível em: <http://www.broadband-forum.org/technical/download/FRF.12/frf12.pdf> Acessado em 06.2007.
- [17] - Emulation, simulation and traffic generation: Disponível em: <http://linuxnet.osdl.org/index.php/Netem> Acesso em 05.2007
- [18]- MGEN - MultiGanerator, Disponível em: <http://computing.ee.ethz.ch/sepp/mgen-3.0-mo> Acesso em:02.06.2006
- [19]- Estrutura de sistemas de arquivos,disponivel em : <http://penta2.ufrgs.br/rc952/trab1/ftp2.html> acesso em julho,2010
- [20] - VoIP over Frame Relay with Quality of Service (Fragmentation, Traffic Shaping, LLQ / IP RTP Priority, Disponível em: http://cisco.com/en/US/tech/tk652/tk698/technologies_configuration_example09186a0080094af9.shtml Acesso em Dez/2010
- [21] – Lu Ruan; Zhi Liu - Upstream Node Initiated Fast Restoration in MPLS Networks;, Department of Computer Science; Iowa State University, Ames, IA 50011 – Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1494492> Acesso em Maio/2009.
- [22] Atsushi Kobayashi, Katsuyasu Toyama, "Method of Measuring VoIP Traffic Fluctuation with Selective sFlow," saint-w, pp.89, 2007 International Symposium on Applications and the Internet Workshops (SAINTW'07), 2007 Disponível em <http://doi.ieeecomputersociety.org/10.1109/SAINT-W.2007.74> Acesso em Fev/2010
- [23] - David D. Clark, MIT Laboratory for Computer Science, Computer Systems and Communications Group, July, 1982 - RFC 815 - IP datagram reassembly algorithms, <http://www.faqs.org/rfcs/rfc815.html> Acesso em Fev 2011.

-
- [24] – RFC 1315 - Brown PS C., F. Baker, C. Carvalho, "Management Information Base for Frame Relay DTEs", disponível em <http://www.rfc-editor.org/in-notes/rfc/files/rfc1315.txt> Acesso em Maio/2006
- [25] – Subramanian, V., Frame Relay Networks, Aug,95, disponível em: http://www1.cse.wustl.edu/~jain/cis788-95/ftp/frame_relay.pdf Acesso em 09.2010
- [26] - D. Hutchison, et all. *Quality of Service Management in Distributed Systems*. M. Sloman ed., "Network and Distributed Systems Management", Addison Wesley, 1994.
- [27] -Ranjbar, Amir S. CCNP ONT *Official Exam Certification Guide* - Cisco Press, CCIE No. 8669 ; 800 East 96th Street - Indianapolis, IN 46240 USA
- [28] - Implementing Quality of Service Policies with DSCP - QoS Packet Marking. Disponível
http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml#expeditedforwarding Acessado em 10.2010
- [29] - ATLAS Frame Relay, User Manual, Part Number 1200263L1-1.1A, Disponível em:
<http://www.optimumdata.com/shop/files/adtran/atlas800/atlas800framerelayusermanual.pdf> Acesso em 10.2010
- [30] – Frame Relay, disponível em: <http://www.protocols.com/pbook/frame.htm>
Acesso em 02.2011
- [31] - *Internetworking Technologies Handbook, Frame relay, chapter 10*, Disponível em: <http://faculty.ccri.edu/tonyrashid/Files/CCNA/frame.pdf> Acesso em 02.2011
Acesso em Fev/2011
- [32] - ITU-T (1996). Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s. ITU-T Recommendation G.723.1, ITU- T, Disponível em: <http://www.ece.cmu.edu/~ece796/documents/g723-1e.pdf> Acesso em Fev/2011
- [33] –ITU-T G.723 - ISO/IEC Disponível em: http://www-1ns.tf.uni-kiel.de/demo/frame_g723.html Acesso em Fev/ 2011
- [34] - ITU-T - INTERNATIONAL TELECOMMUNICATION UNION (1996). Methods for subjective determination of transmission quality. ITU-T Recommendation P.800, ITU-T. Disponível em:
<http://www.catr.cn/radar/itut/201007/P020100707483563647451.pdf> Acesso em Fev/2011
- [35] – Henning Schulzrinne - Audio codecs, 09.12.2008, Disponível em :
<http://www.cs.columbia.edu/~hgs/audio/codecs.html> Acesso em 08 Abril de 2011.
- [36] - Acterna DA-3600 Data Network Analyzer - Advanced IP network troubleshooting and analysis for packet-over-SONET/SDH networks Disponível em:

www.vilcom.ru/files/pdf/Acterna/.../ACTERNA%20DA-3600.pdf Acesso em 16.06.2011

[37] – Robertson, Alex Galhano, Implantando um serviço de telefonia IP em empresas de grande e médio porte – Niteroi, RJ: [s.n.]; 2010, 161f.

[38] - Cisco 1760 Modular Access Router, Disponível em: http://www.cisco.com/en/US/products/hw/routers/ps221/products_data_sheet09186a00800920f2.html#47598 Acesso em 13 de Junho de 2011.

[39] Cisco IP Communications Voice/Fax Network Module. Disponível em: http://www.cisco.com/en/US/prod/collateral/modules/ps5365/product_data_sheet0900aec801c595e_ps259_Products_Data_Sheet.html, acesso em 10 Junho de 2011.

[40] - Digital J1 Packet Voice Network Module, Disponível em: http://www.cisco.com/en/US/products/hw/routers/ps259/products_data_sheet09186a0080088754.html, Acesso em 10 de junho de 2011

[41] - Cisco 2600 Series Multiservice Platforms - Data Compression Advanced Integration Modules. Disponível em: http://www.cisco.com/en/US/prod/collateral/routers/ps274/ps279/product_data_sheet09186a0080091b8a_ps259_Products_Data_Sheet.html Acesso em: 13 Junho 2011.

[42]- Software basic for PBX, disponível em; <http://www.3cx.com.br/voip-sip/fix-fxo.php> Acesso em 13 de Julho de 2011.

9.2 - REFERÊNCIAS CONSULTADAS

[43] – Rey, M. del, Califórnia, RFC 760 - DoD standard Internet Protocol, Jan/1980 , disponível em: <http://www.faqs.org/rfcs/rfc760.html> , Acesso em 20.4.2006

[44] – Clarence, F., E. John, Deploying IP and MPLS QoS for Multiservice Networks – Theory and practice;; Morgan Kaufmann.

[45] - MPLS advantages for traffic engineering
Swallow, G.Communications Magazine, IEEE; Volume 37, Issue 12, Dec 1999
Page(s):54 -57Digital Object Identifier 10.1109/35.809385 Disponível em:
<http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=00809385> Acessado em 02/12/2009.

[46] - RFC 2702 - Requirements for Traffic Engineering Over MPLS
Network Working Group - D. Awduche; J. Malcolm ; J. Agogbua ;M. O'Dell; J. McManus; UUNET (MCI Worldcom) - September 1999. Disponível em:
<http://www.faqs.org/ftp/rfc/pdf/rfc2702.txt.pdf> Acessado em 02 Dezembro 2009

[47] - RFC 2547 - BGP/MPLS VPNs - Network Working Group - E. Rosen; Y. Rekhter; Disponível em: <http://www.rfc-editor.org/rfc/rfc2547.txt> : Acesso em Jul/2009

-
- [48] - Wang, Zheng. “Internet QoS: architecture and mechanisms for quality of service”, Morgan Kaufmann Publishers, New York, 2001.
- [49] - Martins, J. “QoS em Redes IP. Princípios Básicos, Parâmetros e Mecanismos.”, JSMNet Networking Reviews, 1999
- [50]- RFC 3784 - Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)", H. Smit e T. Li, "IS-IS - IETF.
Disponível em <http://www.faqs.org/rfcs/rfc3784.html> . Acesso em Nov/2009
- [51] - Bermond, Antonio Augusto, “Algoritmos de Roteamento para Suporte de Qualidade de Serviço em Aplicações Multimídia”, UFES, Vitória, 2002.
- [52] -Soares, Luiz F. Gomes. “Redes de computadores das LANS, MANS e WANS às redes ATM”, 2.ed., Campus, Rio de Janeiro, 1995
- [53] - Semeria, Chuck, “Supporting Differentiated Service Classes: Queue Scheduling Disciplines”, Juniper Networks, USA, 2001 Disponível em:
http://www.juniper.net/solutions/literature/white_papers/200020.pdf acesso em Julho/2008
Acesso em Dez/2010
- [54] - Técnicas de enfileiramento de QoS – Microsoft Corporation Inc. Disponível em:
<http://support.microsoft.com/kb/233039/pt-br>. Acesso em 12 Jan/2010.
- [55] - Shreedhar, M.; Varghese, G.; “Efficient fair queuing using deficit round-robin”, IEEE-ACM, Transaction on Networking, vol. 4, no. 3, Jun 1996, pp. 375-385.
- [56] - Braden, R.; Clark, D.; Shenker, S.; “Integrated Services in the Internet Architecture: an Overview”, IETF RFC 1633, disponível em
<http://groups.csail.mit.edu/ana/Publications/PubPDFs/Integrated-Services-in-the-Internet-Architecture-rfc1633.txt> Acesso em Dez/2010
- [57] RFC 3031 - Multiprotocol Label Switching Architecture Disponível em
<http://www.faqs.org/rfcs/rfc3031.html> . Acesso em Fev/2010
Network Working Group; Request for Comments: 3031; Category: Standards Track
E. Rosen; A. Viswanathan; R. Callon
- [58] - Heinanen, J.; et al., “Assured Forwarding PHB Group”, IETF RFC 2597, June 1999
Disponível em <http://www.ietf.org/rfc/rfc2597.txt> Acesso em Dez/2010
- [59] - Wroclawski, J.; “Specification of the Controlled-Load Network Element Service”, IETF RFC 2211, 1994, disponível em : <http://www.faqs.org/rfcs/rfc2211.html>
Acesso em Dez/2010
- [60] - Shenker, S.; Partridge, C.; Guerin, R., “Specification of Guaranteed Quality of Service”, disponível em <http://www.faqs.org/rfcs/rfc2212.html> Acesso Junho/2010
- [61] RFC 3032 - MPLS Label Stack Encoding
Disponível em <http://www.faqs.org/rfcs/rfc3032.html> acessado em Dez/2009
Network Working Group; Request for Comments: 3032 ; Category: Standards Track
E. Rosen; D. Tappan; G. Fedorkow; TranSwitch Corporation January 2001

-
- [62] - Boletim bimestral sobre tecnologia de redes produzido e publicado pela RNP – Rede Nacional de Ensino e Pesquisa 12 de maio de 2000 | volume 4, número 3 ISSN 1518-5974 http://www.rnp.br/newsgen/0005/qos_voip1.html#ng-qos Acesso em Dez/2010
- [63] - Bernet, Y.; “Networking Quality of Service and Windows Operating Systems”, New Riders Publishing and Microsoft Corporation, November 2001
- [64] - Silberschatz, A.; et al, “Sistemas Operacionais, conceitos e aplicações”, Editora Campus – Elsevier 2000, Rio de Janeiro - 6ª Tiragem
- [65] - S. Keshav, “An Engineering Approach to Computer Networking”, USA, 1997
- [66] - Cisco Any Transport over MPLS Q&A acessível em: <https://www.cisco.com/en/US/tech/tk436/tk427/technologies.html> Acessado em Jan/2008.
- [67] - Stephen Shew - Traffic Engineering WG, Nortel Networks, October 1999, disponível em <http://tools.ietf.org/html/draft-shew-lsp-restoration-00> Acesso em Dez/2010
- [68] - D. Katz, D. Yeung e K. Kompella, "RFC 3630 - Traffic Engineering (TE) Extensions to OSPF Version 2", IETF, RFC 3630.
Disponível em: <http://www.faqs.org/rfcs/rfc3630.html> Acesso Junho /2010
- [69] - Amiri, N.K.; Fakhraie, S.M.; Hosein-Zadeh, G.-A.; Mousavinejad, S.M.; Sch. of Electr. & Comput. Eng., Univ. of Tehran, Tehran - Modeling of ITU-T G.729 codec with bit-width optimization for intensive computation blocks Disponível em : http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=4497659 Acesso em Maio/2010
- [70] - Oouch, H. et al, NTT Network Syst. Dev. Center, Tokyo, Japan - Study on appropriate voice data length of IP packets for VoIP network adjustment, 26 March 2003, Disponível em : <http://ieeexplore.ieee.org/search/freeseachresult.jsp?newsearch=true&queryText=VoIp+in+network+data> Acesso em Maio/2010.
- [71] - R. Marina del et al, INTERNET PROTOCOL, University of Southern California, September 1981 RFC 791, disponível em : <http://www.faqs.org/ftp/rfc/pdf/rfc791.txt.pdf> Acesso em Dez/2010
- [72] – Telefonia VoIP sobre redes de pacotes em comunicação modernas - <http://www.geocities.com/SiliconValley/Vista/8672/network/ipfrag.html> Acesso em Dez/2010

-
- [73] - J. Mogul et al, Path MTU Discovery, RFC 1191, Stanford University, November 1990,: Disponível em <http://www.faqs.org/rfcs/rfc1191.html> Acesso em Dez/2010
- [74] – David, Bruce S, MPLS: Technology and application; Morgan Kaufmann, 2000 Boston – USA
- [75] - Li Erran et al, Routing Bandwidth Guaranteed Paths With Local Restoration in Label Switched Networks -.Disponível em: -
<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1391048&userType=&tag=1>
 Acesso em Maio/2010.
- [76] – J. Le Roux et al, P2MP MPLS-TE Fast Reroute with P2MP Bypass Tunnels, March 2008 ;, Disponível em: <http://tools.ietf.org/html/draft-ietf-mpls-p2mp-te-bypass-02> Acesso Maio/2010
- [77] – Gallaher R, MPLS Training Guide – Building Multi Protocol Label Switching Network – Your Complete Guide to Signaling and Tunneling Protocols and Traffic Engineering, 2003 – Syngress, USA - MA
- [78] – Dongmei Wang, *Member, IEEE*, and Guangzhi Li, *Member, IEEE* - Efficient Distributed Bandwidth Management for MPLS Fast Reroute. Disponível em: <http://portal.acm.org/citation.cfm?id=1373990.1374009> Acessado em Maio/2009
- [79] – Y. Ohba;Y. Katsube et al, Request for Comments: 3063- MPLS Loop Prevention Mechanism February 2001 Disponível em: <http://www.faqs.org/rfcs/rfc3063.html> Acesso em Maio/2009
- [80] - Minei Ina, Lucek Julian, Wiley – Second Edition, 2008, MPLS – Enabled Applications – Emerging Developments and New Technologies.
- [81] - Tanenbaum, A. S. “Redes de Computadores”, Ed.Campus, 4ª Edição, 2003, Brasil, 11ª Tiragem.
- [82] – Davie B. S., Farrel A. “MPLS : Next Steps”, Margan Kaufmann,2008, II Title, USA
- [83] - V. Jacobson, February 1990, *Compressing TCP/IP Headers for Low-Speed Serial Links*: Disponível em: <http://www.faqs.org/rfcs/rfc1144.html> : Acessado em 06.2007
- [84] - H. Schulzrinne, July 2003, RFC 3550 - RTP: A Transport Protocol for Real-Time Applications.Disponível em : <http://www.faqs.org/rfcs/rfc3550.html> , acesso em 07.2007
- [85] – Alcatel-Lucent_MPLS_Student_Guide_v1-1.pdf Disponível em: <http://www.alcatel-lucent.com/src> Acesso em: Novembro/2008

-
- [86] - RFC3032 - MPLS Label Stack Encoding. Disponível em <http://www.faqs.org/rfcs/rfc3032.html> Acesso em Agosto/2010.
- [87] – *Introduction to Cisco MPLS VPN Technology* - Disponível em: http://www.cisco.com/en/US/docs/net_mgmt/vpn_solutions_center/1.1/user/guide/VPN_UG1.html Acessado em Jan/2010
- [88] - *Codec Summary table*: Disponível em <http://www.en.voipforo.com/codec/codecs.php> Acessado em 06.2007
- [89] - V. Jacobson, January 1996, RFC 1889 - RTP: A Transport Protocol for Real-Time Applications, Disponível em : <http://www.faqs.org/rfcs/rfc1889.html> acesso em 08.2006.
- [90] - ITU-T (1996). Subjective performance assessment of telephoneband and wideband digital codec's. ITU-T Recommendation P.830, ITU- T. Disponível em: <http://www.catr.cn/radar/itut/201007/P020100707481270756128.pdf> Acesso em Fev/2011
- [91]- ITU-T (1990). 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM). ITU-T Recommendation G.726, ITU- T. Disponível em: <http://eu.sabotage.org/www/ITU/G/G0726e.pdf> Acesso em Fev/2011.
- [92] - Toll Quality Voice - 32 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM) MIME Sub-type Registration G. Vaudreuil, Jane 2004. Disponível em: <http://www.itu.int/rec/T-REC-G.729-200701-I/en> Acesso em 08 Abril 2011.
- [93]- G.729: Coding of speech at 8kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP), Disponível em: <http://www.itu.int/rec/T-REC-G.729-199603-S/en> Acesso em 08 de Abril 2011.
- [94] - *MPLS Label Distribution Protocol (LDP) - Cisco IOS Software Releases 12.2*.Disponível: http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/lsldp2s.html#wp1354670 Acessado em Jan/2010.
- [95] - ITU-T (1988). Pulse code modulation (PCM) of voice frequencies. ITU-T Recommendation G.711, ITU-T. Disponível em: <http://www.itu.int/itu-t/recommendations/rec.aspx?id=10653> Acesso em 06.2011.
- [96] – ITU-T Recommendation G.711: Pulse code modulation (PCM) of voice frequencies, 14.03.2011, Disponível em: <http://www.itu.int/rec/T-REC-G.711/e> Acesso em 06 junho 2011.
- [97] - G. Vaudreuil, Toll Quality Voice - 32 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM) MIME Sub-type Registration, June, 2004. Disponível em: <http://tools.ietf.org/html/rfc3802> Acesso em 06 Junho 2011.

-
- [98] - Quality of Service Networking; Disponível em:
<http://www.cisco.com/en/US/docs/internetworking/technology/handbook/QoS.pdf>,
acesso em 06.06.2007
- [99] – RFC – 1771 -A Border Gateway Protocol 4 (BGP-4)- Y. Rekhter, et al , March 1995 - Disponível em: <http://www.faqs.org/rfcs/rfc1771.html> Acesso em Dez/2010
- [100]- MPLS Traffic Engineering Fast Reroute — Link Protection. Disponível em
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st16/fr.htm#14052> Acesso em 10.04.2010.
- [101]- Converged Services over MPLS:Andrew G. Malis; *Tellabs* - IEEE Communications Magazine • September 2006, Disponível em:
<http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=35> Acessado em Jun/2007.
- [102] – RFC 3443- Time To Live (TTL) Processing in Multi-Protocol Label. Disponível em : <http://www.faqs.org/rfcs/rfc3443.html> Acesso em Agosto/2010.
- [103] - <http://datatracker.ietf.org/doc/rfc3036/> Request for Comments: 3036
LDP Specification by L. Andersson et all - Nortel Networks Inc. Acesso Junho /2007

10 - CAPÍTULO X – APÊNDICE I

“Temos a arte para não morrermos por causa da verdade” – Nietzsche

*"Mestre não é quem sempre ensina, mas quem de repente aprende."
João Guimarães Rosa*

Este capítulo (X) é um complemento aos demais e tem por objetivo apresentar algumas telas geradas e capturadas durante os testes, que ajudam a entender e ilustrar todo o trabalho para fins de extração de valores estatísticos.

10.1 - Outros Resultados parciais da compressão de cabeçalho RTP

Serão apresentados outros resultados extraídos dos testes de compressão RTP, com as respectivas telas bem como a interpretação dos protocolos e telas.

10.1.1 Teste com 1 fluxo com e sem compressão

A ilustração da Figura 34 a seguir foi usada para facilitar a interpretação dos resultados que compõem os testes preliminares sobre a compressão de cabeçalho RTP.

Number	DeltaTime	Size	Destination	Source	Interpretation
1		16			DCE T1.617 Annex D STATUS ENQUIRY IE Identifier=Ref
2	960 us	16			DCE T1.617 Annex D STATUS IE Identifier=Ref
3	1.2 sec	50	192.168.0.6	192.168.0.10	TCP D=H.225.0 S=15930 SYN Seq=106426024
4	5.0 ms	50	192.168.0.10	192.168.0.6	TCP D=15930 S=H.225.0 SYN Ack=106426024
5	2.0 ms	46	192.168.0.6	192.168.0.10	TCP D=H.225.0 S=15930 Ack=1508282598 Seq=1508282598
6	9.7 ms	351	192.168.0.6	192.168.0.10	H.225.0 Frame Fragmented SETUP IEI=Bearer
7	39.5 ms	169	192.168.0.10	192.168.0.6	H.225.0 CALL PROCEEDING IEI=User-User U
8	14.4 ms	134	192.168.0.10	192.168.0.6	H.225.0 PROGRESS IEI=Facility Location=
9	25.8 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=679 Timestamp=0 SSR
10	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=680 Timestamp=160 S
11	20.3 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=681 Timestamp=320 S
12	20.1 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=682 Timestamp=480 S
13	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=683 Timestamp=640 S
14	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=684 Timestamp=800 S
15	17.7 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=685 Timestamp=960 S
16	20.3 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=686 Timestamp=1120 S
17	20.1 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=687 Timestamp=1280 S
18	260 us	46	192.168.0.6	192.168.0.10	TCP D=H.225.0 S=15930 Ack=1508282809 Seq=1508282809
19	20.0 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=688 Timestamp=1440 S
20	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=689 Timestamp=1600 S
21	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=690 Timestamp=1760 S
22	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=691 Timestamp=1920 S
23	20.1 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=692 Timestamp=2080 S
24	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=693 Timestamp=2240 S
25	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=694 Timestamp=2400 S
26	20.1 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=695 Timestamp=2560 S
27	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=696 Timestamp=2720 S
28	20.1 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=697 Timestamp=2880 S
29	17.7 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=698 Timestamp=3040 S
30	20.1 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=699 Timestamp=3200 S
31	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=700 Timestamp=3360 S
32	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=701 Timestamp=3520 S
33	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=702 Timestamp=3680 S
34	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=703 Timestamp=3840 S
35	20.2 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=704 Timestamp=4000 S

Figura 34 - Detalhamento adicionais sobre pacotes sem compressão capturados no acesso FR de 512K

Na Figura 34, percebe-se ainda da presença dos protocolos como TCP, usado para estabelecer conexão bem como de outros protocolos *setados* como H.225 para telefonia. Desse teste de compressão, medido usando o CODEC G729 sem compressão de cabeçalho, os pacotes de voz continuam no seu tamanho normal de 66bytes e nos oito minutos de testes a rede teve uma ocupação de 26000bps de acordo com a Tabela 37 – Medição de Compressão com cRTP desabilitado, a seguir extraída da estatística dos últimos 30sec do roteadores cisco de acesso.

```
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
30 second input rate 26000 bits/sec, 50 packets/sec (...)
```

Tabela 37 - Medição de Compressão com cRTP desabilitado.

A Tabela 37, é trecho dos resultados analisados no script da interface de saída dos CPE,s. À semelhança da Figura 34, a Figura 35 a seguir representa a ilustração dos testes de compressão, onde foram comprimidos os cabeçalhos RTP

Number	DeltaTime	Size	Destination	Source	Interpretation
1	960 us	16	DCE	DCE	DCE TL 617 Annex D STATUS ENQUIRY IE Identifier
2	3.0 sec	330	DTE	DCE	DCE TL 617 Annex D STATUS IE Identifier-Report
3	2.4 sec	50	192.168.0.10	192.168.0.6	DCE CDP Name=CPE-02 IP Address=192.168.0.6 Pl
4	3.8 ms	50	192.168.0.6	192.168.0.10	TCP D=H.225.0 S=41760 SYN Seq=1026946729
5	2.4 ms	46	192.168.0.10	192.168.0.6	TCP D=41760 S=H.225.0 SYN Ack=1026946730
6	10.5 ms	351	192.168.0.10	192.168.0.6	TCP D=H.225.0 S=41760 Ack=293904192 Seq=1
7	33.1 ms	169	192.168.0.6	192.168.0.10	H.225.0 Frame Fragmented SETUP IEI=Bearer
8	5.1 ms	134	192.168.0.6	192.168.0.10	H.225.0 CALL PROCEEDING IEI=User-User Use
9	18.9 ms	66	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
10	19.5 ms	31	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
11	20.1 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
12	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
13	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
14	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
15	20.3 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
16	20.1 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
17	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
18	17.7 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
19	17.1 ms	46	192.168.0.10	192.168.0.6	TCP D=H.225.0 S=41760 Ack=293904403 Seq=1
20	3.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
21	20.1 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
22	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
23	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
24	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
25	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
26	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
27	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
28	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
29	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
30	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
31	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
32	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
33	17.6 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
34	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
35	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
36	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
37	20.1 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
38	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non
39	20.2 ms	28	DCE	DTE	DTE Frame Relay DLCI=100 InformationType=Non

Figura 35 - Detalhamento adicionais sobre Pacotes Comprimidos capturados no acesso FR de 512K

Neste teste, o frame passa de 66bytes para 28bytes para cada fluxo de voz, conforme pode ser observado na terceira coluna. A Tabela 38 a seguir representa a capacidade da banda ocupada no teste com a compressão habilitada:

Output queue: high size/max/dropped 0/256/0
Output queue: 0/128 (size/max)
30 second input rate 10000 bits/sec, 50 packets/sec

Tabela 38 - Medição de compressão com cRTP habilitado.

Conforme Tabela 38, os 1000bps representa a ocupação da banda quando ocorre a compressão de cabeçalho para apenas um canal de voz.

10.1.2 – Analise em backbone

No domínio do backbone algumas análises foram realizadas a nível de protocolo, assim como ao nível do tamanho de overhead que cada fluxo carrega.

10.1.2.1 - Analise de compressão RTP a nível backbone.

A Figura 36 a seguir ilustra um pacote capturado da chamada realizada do CPE02 (192.168.0.6) ramal 3000 para o CPE03 (192.168.0.10) ramal 5000.

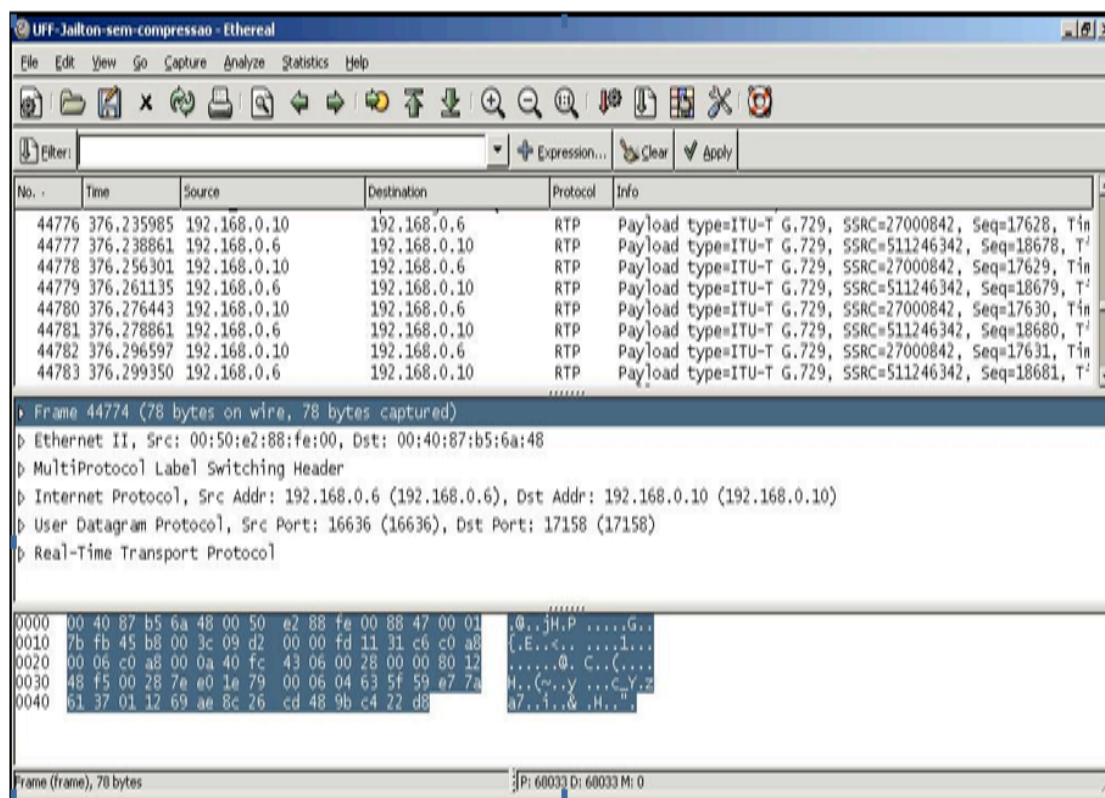


Figura 36 - Pacote sem compressão no Backbone IP/MPLS

Pode-se observar no pacote capturado que foram designados dois SSRC um no sentido 192.168.0.6 para 192.168.0.10 e outro no sentido inverso; pode-se notar,

também, os números de sequência, o tipo de CODEC, o tempo em que foram gerados, marcações essenciais para aplicações que utilizam RTP.

A Figura 37 - a seguir, representa mais informações do frame do pacote no backbone.

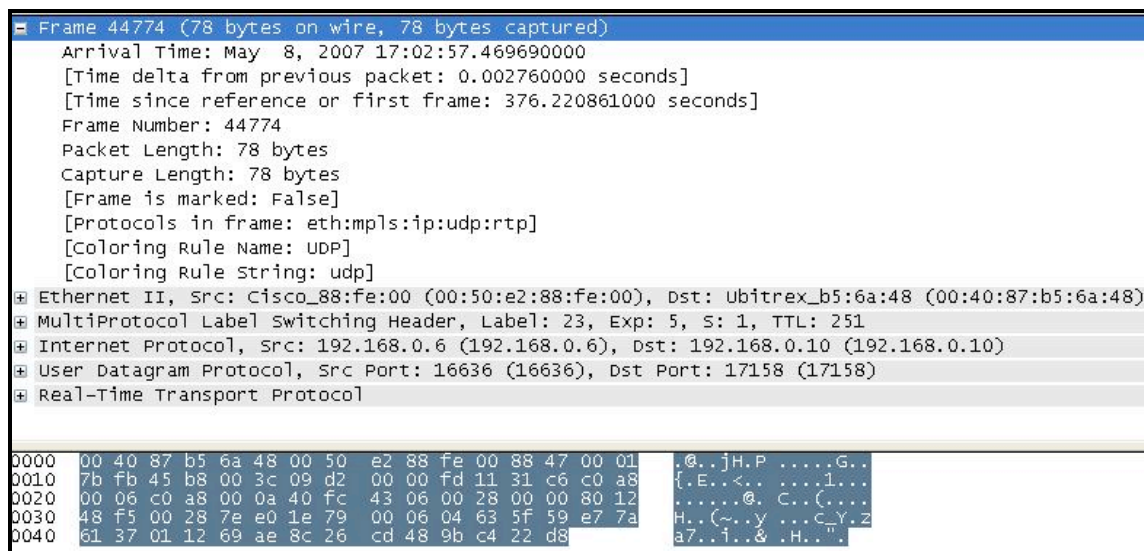


Figura 37 - Informações do Frame capturados no acesso Backbone - MPLS

A partir da Figura 37, pode-se observar que o FRAME no BACKBONE contém 78 bytes, no seu interior tem-se os protocolos Ethernet, MPLS, IP, UDP e RTP e seus *headers* são distribuídos da seguinte forma:

- ✓ Protocolo Ethernet – 14 bytes de header
- ✓ Protocolo MPLS – 4 bytes de header
- ✓ Protocolo IP – 20 bytes de header
- ✓ Protocolo UDP – 8 bytes de header
- ✓ Protocolo RTP – 12 bytes de header
- ✓ Payload – 20 bytes

No backbone IP/MPLS os 78 bytes dividem-se em 58bytes de header e apenas 20bytes de payload, ou seja, teremos 74.36% de *overhead* (cabeçalho) e apenas 25,64% de informação útil. Como teoricamente o backbone tem banda suficiente, não existe preocupação em realizar a compressão nesse ambiente.

Esse trabalho é realizado nos gargalos, neste caso, no acesso Frame Relay de 512Kbps do CPE até o roteador de borda. Na seção que se segue, serão analisados cada um desses pacotes, começando pelo *Ethernet*.

10.1.2.2 - Pacote ETHERNET

```

Ethernet II, Src: 00:50:e2:88:fe:00, Dst: 00:40:87:b5:6a:48
  Destination: 00:40:87:b5:6a:48 (Ubitrex_b5:6a:48)
  Source: 00:50:e2:88:fe:00 (Cisco_88:fe:00)
  Type: MPLS label switched packet (0x8847)
  MultiProtocol Label Switching Header
  Internet Protocol, Src Addr: 192.168.0.6 (192.168.0.6), Dst Addr: 192.168.0.10 (192.168.0.10)
  User Datagram Protocol, Src Port: 16636 (16636), Dst Port: 17158 (17158)
  Real-Time Transport Protocol

0000  00 40 87 b5 6a 48 00 50 e2 88 fe 00 88 47 00 01  .@..jH.P ....G..
0010  7b fb 45 b8 00 3c 09 d2 00 00 fd 11 31 c6 c0 a8  {E..<.. ....l...
0020  00 06 c0 a8 00 0a 40 fc 43 06 00 28 00 00 80 12  .....@. C..(....
0030  48 f5 00 28 7e e0 1e 79 00 06 04 63 5f 59 e7 7a  H..(~..y ...c_Y.z
0040  61 37 01 12 69 ae 8c 26 cd 48 9b c4 22 d8      a7..i..& .H..".
  
```

Figura 38 - Pacote Ethernet - análise a partir de backbone IP / MPLS

Na Figura 38, visualiza-se o pacote Ethernet de 14 bytes de header; no seu interior temos o MAC do roteador de origem e destino do backbone, o payload composto pelos pacotes headers MPLS/IP/UDP/RTP+dados somando 64 bytes.

10.1.2.3 - Pacotes MPLS

```

MultiProtocol Label Switching Header
  MPLS Label: Unknown (23)
  MPLS Experimental Bits: 5
  MPLS Bottom Of Label Stack: 1
  MPLS TTL: 251
  Internet Protocol, Src Addr: 192.168.0.6 (192.168.0.6), Dst Addr: 192.168.0.10 (192.168.0.10)
  User Datagram Protocol, Src Port: 16636 (16636), Dst Port: 17158 (17158)
  Real-Time Transport Protocol

0000  00 40 87 b5 6a 48 00 50 e2 88 fe 00 88 47 00 01  .@..jH.P ....G..
0010  7b fb 45 b8 00 3c 09 d2 00 00 fd 11 31 c6 c0 a8  {E..<.. ....l...
0020  00 06 c0 a8 00 0a 40 fc 43 06 00 28 00 00 80 12  .....@. C..(....
0030  48 f5 00 28 7e e0 1e 79 00 06 04 63 5f 59 e7 7a  H..(~..y ...c_Y.z
0040  61 37 01 12 69 ae 8c 26 cd 48 9b c4 22 d8      a7..i..& .H..".
  
```

Figura 39 -Pacote MPLS

Na Figura 39, pode-se perceber o pacote MPLS com 4 bytes de header; nele identificamos o label do próximo roteador MPLS da rede, o TTL do MPLS mais payload composto pelos headers IP/UDP/RTP+dados somando 60 bytes.

10.1.2.4 - PACOTE IP

```

Internet Protocol, Src Addr: 192.168.0.6 (192.168.0.6), Dst Addr: 192.168.0.10 (192.168.0.10)
  Version: 4
  Header length: 20 bytes
  ▸ Differentiated Services Field: 0xb8 (DSCP 0x2e: Expedited Forwarding; ECN: 0x00)
  Total Length: 60
  Identification: 0x09d2 (2514)
  ▸ Flags: 0x00
  Fragment offset: 0
  Time to live: 253
  Protocol: UDP (0x11)
  Header checksum: 0x31c6 (correct)
  Source: 192.168.0.6 (192.168.0.6)
  Destination: 192.168.0.10 (192.168.0.10)
  ▸ User Datagram Protocol, Src Port: 16636 (16636), Dst Port: 17158 (17158)
  ▸ Real-Time Transport Protocol
0000  00 40 87 b5 6a 48 00 50 e2 88 fe 00 88 47 00 01  .@..jH.P....G..
0010  7b fb 45 b8 00 3c 09 d2 00 00 fd 11 31 c6 c0 a8  {.E..<...1...
0020  00 06 c0 a8 00 0a 40 fc 43 06 00 28 00 00 80 12  ....@.C..C...
0030  48 f5 00 28 7e e0 1e 79 00 06 04 63 5f 59 e7 7a  H..(..y...C.Y.z
0040  61 37 01 12 69 ae 8c 26 cd 48 9b c4 22 d8      a7..i..& .H..".

```

Figura 40 - Pacote IP

A Figura 40 exibe-se o pacote IP de 20bytes de cabeçalho, contendo no seu interior o endereço de origem e destino; o tamanho total do datagrama são 60bytes mais payload composto pelos headers UDP/RTP+dados perfazendo 40 bytes.

10.1.2.5 - PACOTE UDP

```

User Datagram Protocol, Src Port: 16636 (16636), Dst Port: 17158 (17158)
  Source port: 16636 (16636)
  Destination port: 17158 (17158)
  Length: 40
  Checksum: 0x0000 (none)
  ▸ Real-Time Transport Protocol
0000  00 40 87 b5 6a 48 00 50 e2 88 fe 00 88 47 00 01  .@..jH.P....G..
0010  7b fb 45 b8 00 3c 09 d2 00 00 fd 11 31 c6 c0 a8  {.E..<...1...
0020  00 06 c0 a8 00 0a 40 fc 43 06 00 28 00 00 80 12  ....@.C..C...
0030  48 f5 00 28 7e e0 1e 79 00 06 04 63 5f 59 e7 7a  H..(..y...C.Y.z
0040  61 37 01 12 69 ae 8c 26 cd 48 9b c4 22 d8      a7..i..& .H..".

```

Figura 41 - Pacote UDP

Na Figura 41, vê-se o pacote UDP que possui 8 bytes de *header*; nele identificamos a porta origem e destino, *checksum* que neste caso não é utilizado, tamanho total de 40 bytes mais *payload* formado pelo *header* RTP+dados somando 32 bytes.

10.1.2.6 - PACOTE RTP

Real-Time Transport Protocol															
10.. = Version: RFC 1889 Version (2)															
..0. = Padding: False															
...0 = Extension: False															
.... 0000 = Contributing source identifiers count: 0															
0... = Marker: False															
.001 0010 = Payload type: ITU-T G.729 (18)															
Sequence number: 18677															
Timestamp: 2653920															
Synchronization Source identifier: 511246342															
Payload: 04635F59E77A6137011269AE8C26CD48...															
0000	00	40	87	b5	6a	48	00	50	e2	88	fe	00	88	47	00 01
0010	7b	fb	45	b8	00	3c	09	d2	00	00	fd	11	31	c6	c0 a8
0020	00	06	c0	a8	00	0a	40	fc	43	06	00	28	00	00	80 12
0030	48	f5	00	28	7e	e0	1e	79	00	06	04	63	5f	59	e7 7a
0040	61	37	01	12	69	ae	8c	26	cd	48	9b	c4	22	d8	

Figura 42 - Pacote RTP

Conforme a Figura 42 em apreço, uma vez retirados os *headers* (cabeçalhos) dos protocolos Ethernet, MPLS, IP e UDP, resta apenas o pacote RTP que transporta em seu *header* o tipo de CODEC, número de sequência, timestamp, SSRC que somados chegam a 12 bytes mais os dados da conversação de 20 bytes. Dessa forma, chegamos ao último nível da informação transmitida.

10.1.2.7 - Pacotes do teste com 2 fluxos de voz com e sem compressão

Nesse exemplo de fluxos em paralelo, foram realizadas as seguintes chamadas:

CPE02 (192.168.0.6) ramal 3000 para o CPE03 (192.168.0.10) ramal 5000

CPE02 (192.168.0.6) ramal 4000 para o CPE03 (192.168.0.10) ramal 6000

Assim como ocorreu nos testes com um único fluxo, nos testes realizados com dois fluxos os pacotes no BACKBONE IP/MPLS apresentaram-se de maneira semelhante uma vez que não ocorreu a compressão no backbone.

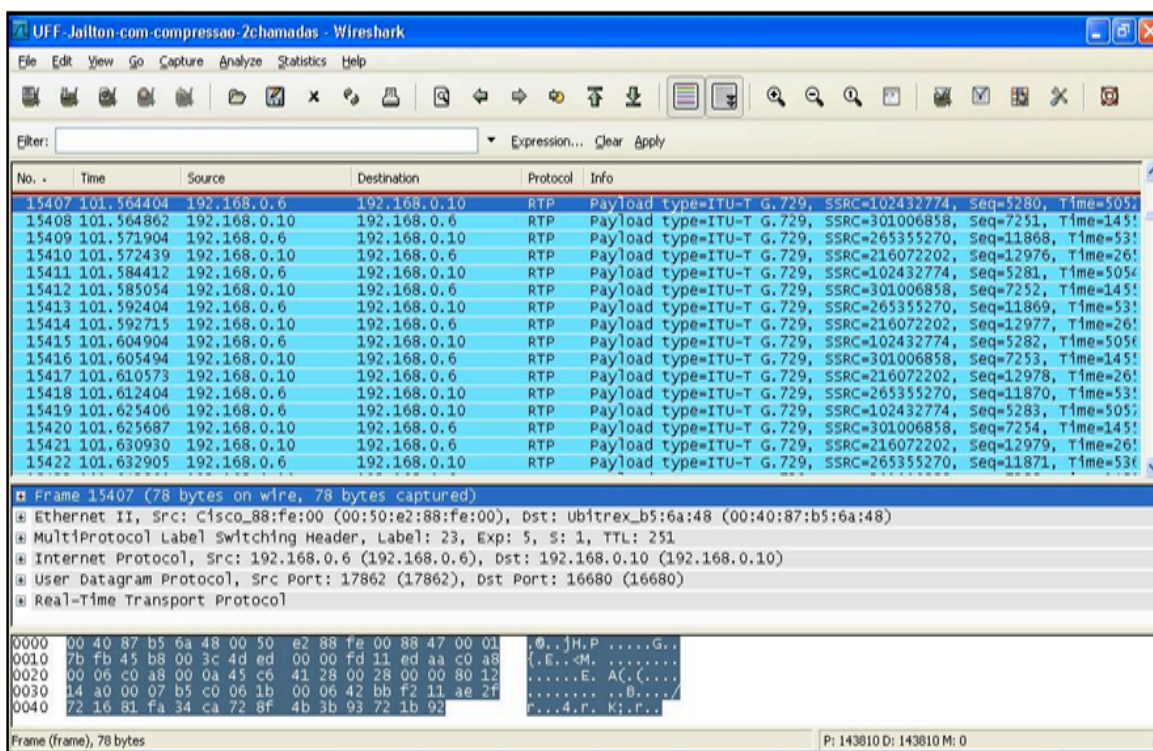


Figura 43 - Testes com dois fluxos de voz no backbone IP/MPLS

De acordo com a Figura 43 foram gerados 4 (quatro) fluxos distintos (dois em cada sentido) tendo cada um assumido um SSRC diferente e cada fluxo transportou a mesma quantidade de informação, conforme já referido anteriormente, ou seja, 78 bytes, sendo 58 de *header* e 20 bytes de informação útil. No tráfego usando dois ramais telefônicos, foi também analisado o tamanho da ocupação da banda - vide Tabela 39 a seguir.

```
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: dual fifo
Output queue: high size/max/dropped 0/256/0
Output queue: 0/128 (size/max)
30 second input rate 20600 bits/sec, 50 packets/sec
30 second output rate 20600 bits/sec, 50 packets/sec
362554 packets input, 2495313 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Tabela 39 - Tamanho da banda ocupada em medição com dois pares de ramais telefônicos.

Na Tabela 39, consta-se que nas mesmas condições de testes de compressão de cabeçalho anteriormente realizados, com dois ramais telefônicos em paralelo, conseguiu-se uma média de ocupação de banda na ordem de 20,6kbps, pois, parte do pressuposto que nos frames de voz foi comprimido o cabeçalho.

10.1.3 - Pacote RTCP capturado no teste com dois fluxos comprimidos

A Figura 44 a seguir mostra as informações dos pacotes RTCP no acesso do backbone IP/MPLS.

No.	Time	Source	Destination -	Protocol	Info
123737	570.867940	192.168.0.6	192.168.0.10	RTP	Payload type=ITU-T G.729, SSRC=265355270, Seq=35333,
123739	570.875930	192.168.0.6	192.168.0.10	RTCP	Receiver Report Source description
123740	570.880971	192.168.0.6	192.168.0.10	RTP	Payload type=ITU-T G.729, SSRC=102432774, Seq=28746,

+	Frame 123739 (158 bytes on wire, 158 bytes captured)
+	Ethernet II, Src: Cisco_88:fe:00 (00:50:e2:88:fe:00), Dst: Ubitrex_b5:6a:48 (00:40:87:b5:6a:48)
+	MultiProtocol Label Switching Header, Label: 23, Exp: 5, S: 1, TTL: 251
+	Internet Protocol, Src: 192.168.0.6 (192.168.0.6), Dst: 192.168.0.10 (192.168.0.10)
+	User Datagram Protocol, Src Port: 16555 (16555), Dst Port: 16633 (16633)
+	Real-time Transport Control Protocol (Receiver Report)
+	[Stream setup by H245 (frame 1276)]
+	10.. = Version: RFC 1889 Version (2)
+	..0. = Padding: False
+	...0 0001 = Reception report count: 1
+	Packet type: Receiver Report (201)
+	Length: 7
+	Sender SSRC: 265355270
+	Source 1
+	Real-time Transport Control Protocol (Source description)
+	[Stream setup by H245 (frame 1276)]
+	10.. = Version: RFC 1889 Version (2)
+	..0. = Padding: False
+	...0 0001 = Source count: 1
+	Packet type: Source description (202)
+	Length: 19
+	Chunk 1, SSRC/CSRC 265355270
+	[RTCP frame length check: OK - 112 bytes]

0010	7b f8 45 88 00 8c 00 6b	00 00 fe 11 39 dd c0 a8	{.E....k ...9...
0020	00 06 c0 a8 00 0a 40 ab	40 f9 00 78 ea 4d 81 c9@. @..x.M...
0030	00 07 0f d1 00 06 0c e1	00 0a 00 00 00 00 00 00
0040	8e 59 00 00 01 e0 87 65	c2 39 00 06 86 24 81 ca	Y.....e 9...\$.
0050	00 13 0f d1 00 06 01 11	30 2e 30 2e 30 40 31 39 0.0.0019
0060	32 2e 31 36 38 2e 30 2e	36 02 17 43 69 73 63 6f	2.168.0. 6..Cisco
0070	20 49 4f 53 2c 20 56 6f	49 50 20 47 61 74 65 77	IOS, Vo IP Gatew
0080	61 79 06 17 43 69 73 63	6f 20 49 4f 53 2c 20 56	ay..Cisco o IOS, v
0090	6f 49 50 20 47 61 74 65	77 61 79 00 00 00	oIP Gate way...

Figura 44 - Pacotes RTCP capturados no backbone IP/MPLS

Na Figura 44, pode-se observar que durante a troca de pacotes RTP também foram enviadas mensagens RTCP; em destaque mostramos os pacotes SR (*Sender Report*) que contêm informações de transmissão e recepção para transmissores ativos e pacotes RR (*Receiver Reports*) que contêm informações de recepção por ouvintes que não sejam também transmissores ativos já mencionados na teoria.

10.2 - MGEN DETALHAMENTOS ADICIONAIS

Nesta seção MGEN, são abordadas algumas questões relacionadas com o uso do gerador MGEN e como são representados os pacotes gerados por este no Acterna. Serão também analisados parâmetros como delay, jitter, perda a partir do coletor do próprio MGEN.

10.2.1 - Script MGEN - Controle e Moldagem de Tráfego em FRF.12 – sem QoS garantida.

```
#Um exemplo de nao cumprimento das politicas basicas de QoS
#Excedendo o CIR e o BC

START NOW
PORT 6000
INTERFACE eth0
TTL 10

# time flowid ON addr:port pattern rate size [RSUP ???] [TOS XX]

# Fluxo 1: voz - CODEC G.711
00000 1 ON 10.20.0.2:5000 PERIODIC 20.0 160 #consume em BW(Banda)=25,6kbps
#00000 1 ON 10.20.0.2:5000 PERIODIC 500.0 700

# Fluxo 2: video
00000 2 ON 10.20.0.2:5001 PERIODIC 30.0 1700 #consume em BW=408kbps

# Fluxo 3: dados
00000 3 ON 10.20.0.2:5002 PERIODIC 50.0 5200 #BW=2,08Mbps; Pkts=500;T=10s
#00000 3 ON 10.20.0.2:5000 PERIODIC 20.0 4000

10000 1 OFF
10000 2 OFF
10000 3 OFF
# o caracter ~#~ significa comentario para aquela linha

# Example line to set IP header TOS bits to a given value (Linux, FreeBSD & NetBSD)
#00000 1 ON 132.250.95.23:5000 PERIODIC 10.0 128 TOS 24
```

Figura 45 – Detalhamento adicionais sobre o Script MGEN - Controle e Moldagem de Tráfego em FRF.12.

Na Figura 46 a seguir, pode-se constatar os endereços IP e a porta de origem e destino, primeiro fluxo indicado pelo seu ID: “Flow 0001” e os demais dados de estatística. Conforme a Figura 46 a percentagem de perda, foi calculado baseado no fato de que dos 200 pacotes transmitidos do fluxo de voz (20pps * 10s), 116 foram descartados e apenas 84 pacotes foram recebidos, sendo que os demais fluxos sequer entraram na interface. Esses valores de estatísticas podem ser notados na ilustração seguinte – Figura 46, extraído do próprio MGEN.

```

root@formica:~# ./nccalc 6PFluxo01D18WQoS_Class
NCCALC: Version 3.3a4

FLOW: 0001 SOURCE: 10.10.0.2:6000 DESTINATION: 10.20.0.2:5000
  Num pkts recvd : 83
  Join delay : 72167.688 sec
  Recv pkt rate : 7.684 pkt/sec
  Recv data rate : 9.955 kbps
  Pkts dropped : 116
  Ave. Tx Delay : 0.963 sec
  Max. Tx Delay : 2.879 sec
  Min. Tx Delay : 0.156 sec
  Delay variation : 2.722 sec

NCCALC: SUMMARY RESULTS
NCCALC: Number of active flows : 1 flows
NCCALC: Number of groups joined : 0 groups

NCCALC: GROUP JOIN LATENCY STATISTICS
NCCALC: Ave. group join latency : 72167.688 sec
NCCALC: Min. group join latency : 72167.688 sec
NCCALC: Max. group join latency : 72167.688 sec

NCCALC: DATA TRANSMISSION LATENCY STATISTICS (Time-sync'd machines required!)
NCCALC: Ave. data latency : 0.963 sec
NCCALC: Min. data latency : 0.156 sec
NCCALC: Max. data latency : 2.879 sec

NCCALC: PER-FLOW DATA LATENCY VARIATION
NCCALC: Ave. latency variation : 2.722 sec
NCCALC: Min. latency variation : 2.722 sec
NCCALC: Max. latency variation : 2.722 sec

NCCALC: PACKET RECEPTION STATISTICS
NCCALC: Total packets received : 83 pkts
NCCALC: Total recv packet rate : 7.684 pkt/sec
NCCALC: Total recv data rate : 9.955 kbps
NCCALC: Est. num pkts dropped : 116 pkts
root@formica:~#

```

Figura 46 - Detalhamento adicionais sobre o Controle e Moldagem de Tráfego em Frame Relay – “QoS não garantida”

Notou-se que a sequência dos fluxos não é necessariamente linear, não comprometendo a eficácia e a viabilidade da aplicação; concluiu-se que, a ordem de intercalação não precisa de ser necessariamente linear, ou seja, na ordem: “RTP – UDP - RPT – Fragmento Frame Relay” (vide Figura 47 a seguir); o tráfego é gerenciado e conformado a se intercalar sempre que houver necessidade sem fugir às normas recomendadas para uma boa aplicação desde que sejam implementadas e respeitadas as normas de QoS.

Da interpretação feita à Figura 47 as seguir, percebe-se que os resultados com relação as variações de retardo foram bastante diferentes dos resultados verificados na Figura 46 anterior, pois, para o caso retratado na Figura 47 foi aplicado QoS e LFI.

DeltaTime	Size	Destination	Source	Interpretation
10.9 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
15.8 ms	648	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
3.1 ms	194	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info
10.8 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info
10.7 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info
12.3 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
3.1 ms	194	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info
10.8 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
3.1 ms	194	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info
10.5 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
3.1 ms	194	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info
10.6 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info
10.6 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
3.1 ms	194	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info
10.7 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
4.1 ms	194	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info
10.2 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
3.5 ms	194	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info
10.2 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
10.2 ms	648	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
11.2 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
6.3 ms	398	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
10.7 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
3.1 ms	194	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
10.5 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
3.1 ms	194	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Len=168
6.3 ms	398	10.10.0.2	10.20.0.2	DTE Frame Relay DLCI=100 InformationType=Non D channel user info

Figura 47 - Aplicação de LFI a rede de pacotes com frame de voz - simulado pelo MGEN

Percebe-se ainda na Figura 47 que, com relação às variações de atraso (*DeltaTime*), indicadas na primeira coluna da ilustração, os valores de jitter foram simplesmente aceitáveis como sendo valores dentro dos limites recomendados. Na terceira linha ainda dessa coluna um nota-se o maior valor de variação de retardo na ordem de 15.8ms, considerado ainda assim um valor abaixo do máximo recomendado que seria os 20ms.

10.3 – ACTERNA

Nesta seção são apresentados detalhes de algumas telas capturadas nos testes de LFI, alguns detalhes das telas provenientes do Acterna Examine nos demais testes.

10.3.1 - Detalhes a nível dos protocolos e QoS apresentados com saída do Acterna

Na Figura 48 constata-se parte de um fluxo ftp cujos parâmetros foram: um *payload* de 1000bytes reproduzidos a uma taxa de 50pps durante 120 000,00 ms. Portanto, é apenas um trecho para ilustrar o resultado do experimento prático. Entendeu-

se ser desnecessária a ilustração de toda a “amostragem”. Consta-se, ainda, que a intercalação para este caso em particular não ocorreu de forma uniforme, já que os pacotes nem sempre foram intercalados na ordem certa, ou seja, houve, em alguns casos, duas sequências seguidas do mesmo fluxo. Isso foi comprovado normal de ocorrer desde que não prejudique a viabilidade do tráfego de tempo real, pelo que pode ser concluído ao verificar o jitter dos fluxos de voz e o tempo utilizado para serialização dos pacotes na entrada e saída das interfaces que registraram um jitter médio de 10ms. Este valor abaixo de 10ms é considerado ótimo, já que a recomendação aceita 20ms a 30ms.

DeltaTime	Size	Destination	Source	Interpretation
10.9 ms	648	10.10.0.2	10.20.0.2	UDP D-COMPLEX MAIN S-X Windows Len=168
6.3 ms	398	10.10.0.2	10.20.0.2	UDP D-COMPLEX LINK S-X Windows Len=1008
15.8 ms	648	10.10.0.2	10.20.0.2	Frame Relay DTE InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D-COMPLEX LINK S-X Windows Len=1008
3.1 ms	194	10.10.0.2	10.20.0.2	Frame Relay DTE InformationType=Non D channel user info
10.8 ms	648	10.10.0.2	10.20.0.2	UDP D-COMPLEX MAIN S-X Windows Len=168
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D-COMPLEX LINK S-X Windows Len=1008
6.3 ms	398	DCE	10.20.0.2	Frame Relay DTE InformationType=Non D channel user info
10.7 ms	648	10.10.0.2	10.20.0.2	UDP D-COMPLEX MAIN S-X Windows Len=168
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D-COMPLEX LINK S-X Windows Len=1008
6.3 ms	398	DCE	10.20.0.2	Frame Relay DTE InformationType=Non D channel user info
12.3 ms	648	10.10.0.2	10.20.0.2	UDP D-COMPLEX MAIN S-X Windows Len=168
6.3 ms	398	DCE	10.20.0.2	UDP D-COMPLEX LINK S-X Windows Len=1008
10.8 ms	648	10.10.0.2	10.20.0.2	Frame Relay DTE InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D-COMPLEX MAIN S-X Windows Len=168
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D-COMPLEX LINK S-X Windows Len=1008
10.5 ms	648	10.10.0.2	10.20.0.2	Frame Relay DTE InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D-COMPLEX MAIN S-X Windows Len=168
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D-COMPLEX LINK S-X Windows Len=1008
10.6 ms	648	10.10.0.2	10.20.0.2	Frame Relay DTE InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D-COMPLEX MAIN S-X Windows Len=168
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D-COMPLEX LINK S-X Windows Len=1008
10.7 ms	648	10.10.0.2	10.20.0.2	Frame Relay DTE InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D-COMPLEX MAIN S-X Windows Len=168
4.1 ms	194	10.10.0.2	10.20.0.2	UDP D-COMPLEX LINK S-X Windows Len=1008
10.2 ms	648	10.10.0.2	10.20.0.2	Frame Relay DTE InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D-COMPLEX MAIN S-X Windows Len=168
3.5 ms	194	10.10.0.2	10.20.0.2	UDP D-COMPLEX LINK S-X Windows Len=1008
10.2 ms	648	10.10.0.2	10.20.0.2	Frame Relay DTE InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D-COMPLEX MAIN S-X Windows Len=168
11.2 ms	648	10.10.0.2	10.20.0.2	UDP D-COMPLEX LINK S-X Windows Len=1008
6.3 ms	398	DCE	10.20.0.2	Frame Relay DTE InformationType=Non D channel user info
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D-COMPLEX MAIN S-X Windows Len=168
10.7 ms	648	10.10.0.2	10.20.0.2	UDP D-COMPLEX LINK S-X Windows Len=1008
3.1 ms	194	10.10.0.2	10.20.0.2	Frame Relay DTE InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D-COMPLEX MAIN S-X Windows Len=168
10.5 ms	648	10.10.0.2	10.20.0.2	UDP D-COMPLEX LINK S-X Windows Len=1008
3.1 ms	194	10.10.0.2	10.20.0.2	Frame Relay DTE InformationType=Non D channel user info
6.3 ms	398	DCE	10.20.0.2	UDP D-COMPLEX MAIN S-X Windows Len=168

Figura 48 - Detalhamento adicionais da Fragmentação Interleaving com QoS e LFI

As Figuras 49 e 50 a seguir representam os detalhes da Figura 48. A Figura 49 mostra estatística ao nível de Frame Relay e IP e os parâmetros referentes a cada protocolo destacados nas cores amarela e rosa. No entanto, as figuras seguintes contêm os demais parâmetros complementares e as informações de outros protocolos.

Ainda na Figura 49 a seguir percebe-se na linha destacada na cor azul que, o fluxo UDP endereço origem 10.20.0.2 e destino 10.10.0.2, tamanho de datagrama de 194bytes e variação do atraso de 3,1ms, apresenta as informações do protocolo Frame

Relay e IP abaixo na mesma Figura 49 e na Figura 50 que se segue serão mostradas as informações dos demais protocolos.

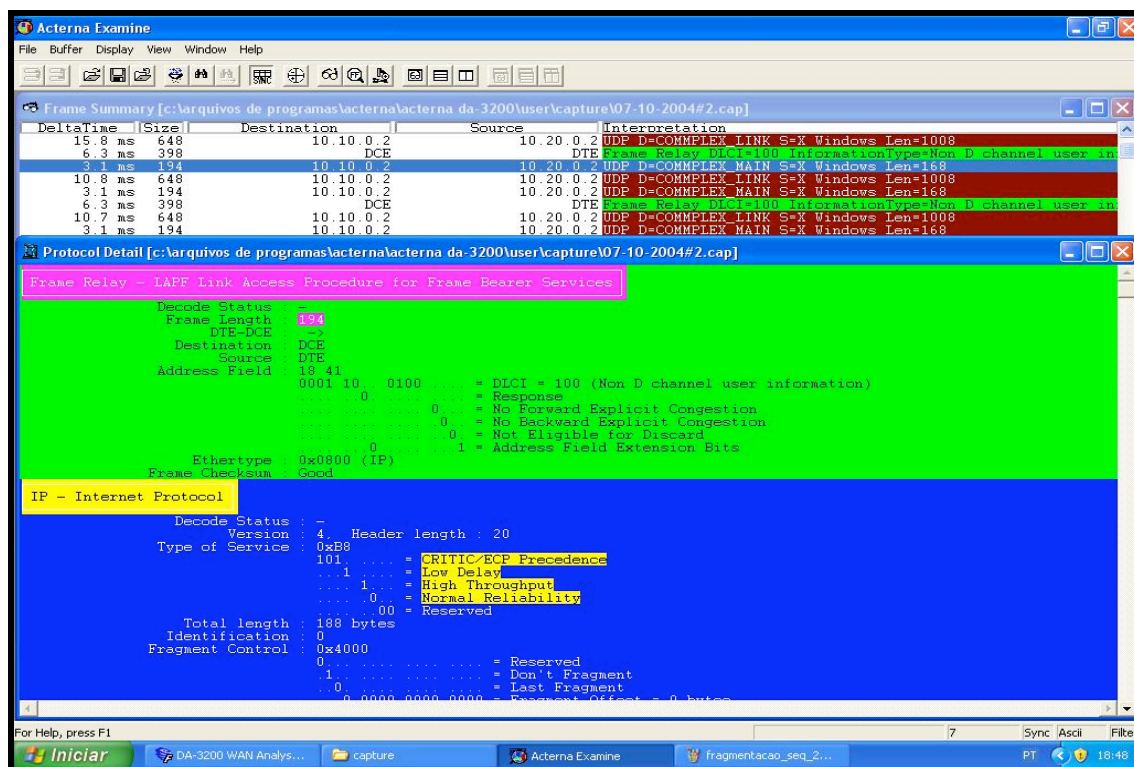


Figura 49 - Detalhes do fluxo de Voz_1 de 2 a nível de protocolos Frame relay e IP.

Dentre algumas informações referentes aos dois protocolos iniciais - IP e Frame Relay - percebe-se o tamanho de frame – 194bytes, frame *checksum* – *good*, DTE fonte e DCE destino, entre outros detalhes do protocolo conforme a figura. Já para o protocolo IP, percebe-se que o bit do controle de fragmento está setado para 1 (um) que equivale a “*don't fragment*”, ToS (Type of Service) setados para baixo *delay*, alto *throughput*, entre outros aspectos relevantes que possam ser verificados na Figura 49.

Na Figura 50 a seguir (segunda parte dos detalhes dos protocolos de datagrama UDP de voz) verificam-se os detalhes do protocolo UDP, indicando além do tamanho do pacote os endereços de origem e de destino, conforme mostram os detalhes do citado protocolo circundados com a cor verde, pois, são as portas setadas no gerador MGEN e o pacote de *payload* 160 bytes acrescido de 8 bytes de cabeçalho do protocolo em análise.

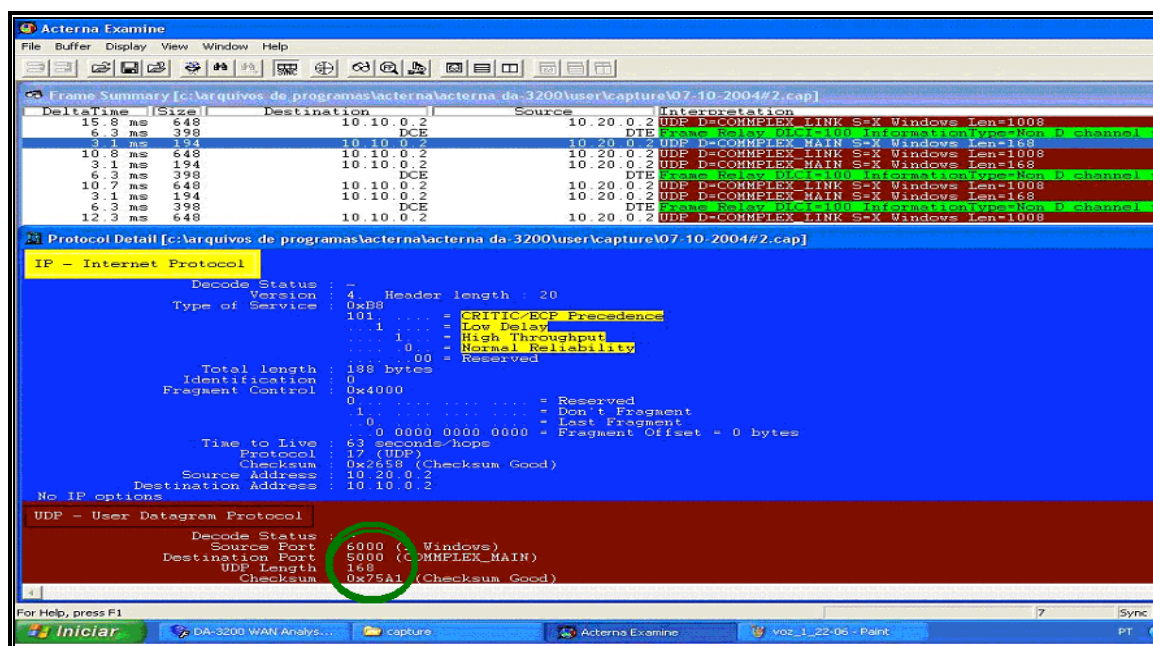


Figura 50 - Detalhes do fluxo de Voz_2 de 2 a nível de protocolos IP e UDP

A Figura 50 representa os detalhes da parte dois dos pacotes de classe voz, que são intercalados entre os pacotes de dados fragmentados. Portanto, as próximas figuras apresentam as três figuras sendo que a primeira - Ilustração Business_1 de 2 é o pacote referente ao máximo valor da MTU = 640 bytes (mais 8bytes UDP) cujo número de sequência é 146 e a próxima sequência o número é 147 e diz respeito ao fragmento restante de fragmento resultante (Ilustração Business_2 de 2) a nível de FRF.12, conforme indica a Figura 51: *Fragmented Protocol over Frame Relay*, destacado na cor rosa.

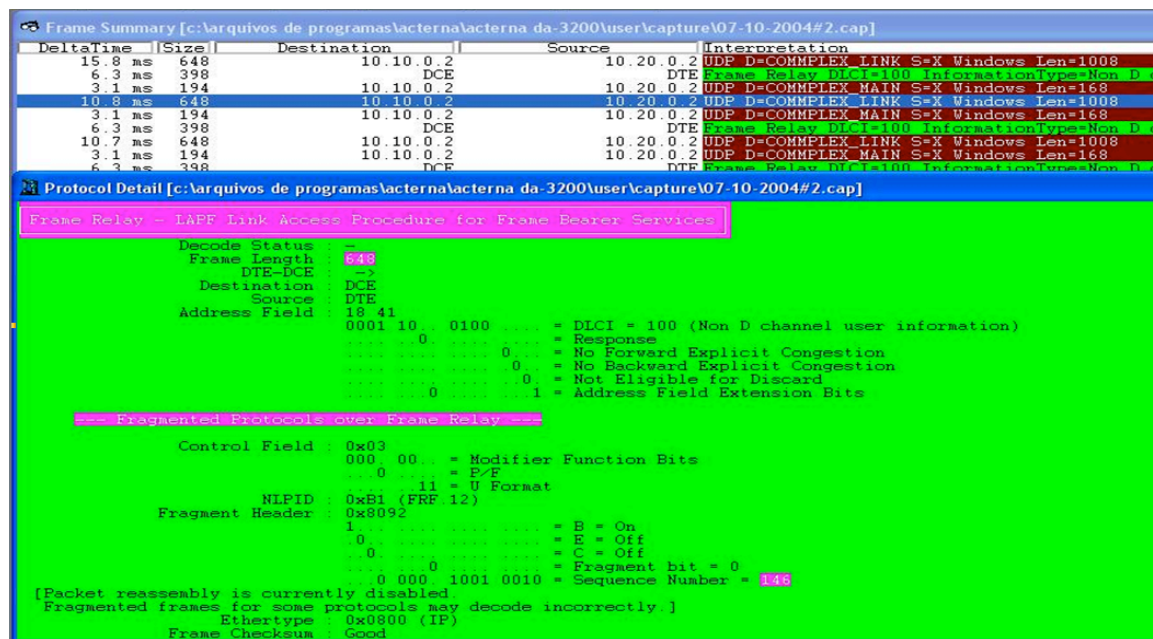


Figura 51 - Detalhes do fluxo classe business_1 de 2 tamanho do fragmento e nº seqüência.

As análises das informações desses protocolos são referentes ao fluxo de classe business destacado na cor azul, com jitter de 10.8 ms, size de 648bytes concernente ao primeiro fragmento, endereço de destino 10.10.0.2 e endereço de origem de 10.20.0.2. A Figura 52 a seguir representa os detalhes do IP e UDP para a mesma classe business. Nesta classe, contrariamente a classe de voz, o parâmetro de atraso é setado como sendo normal.

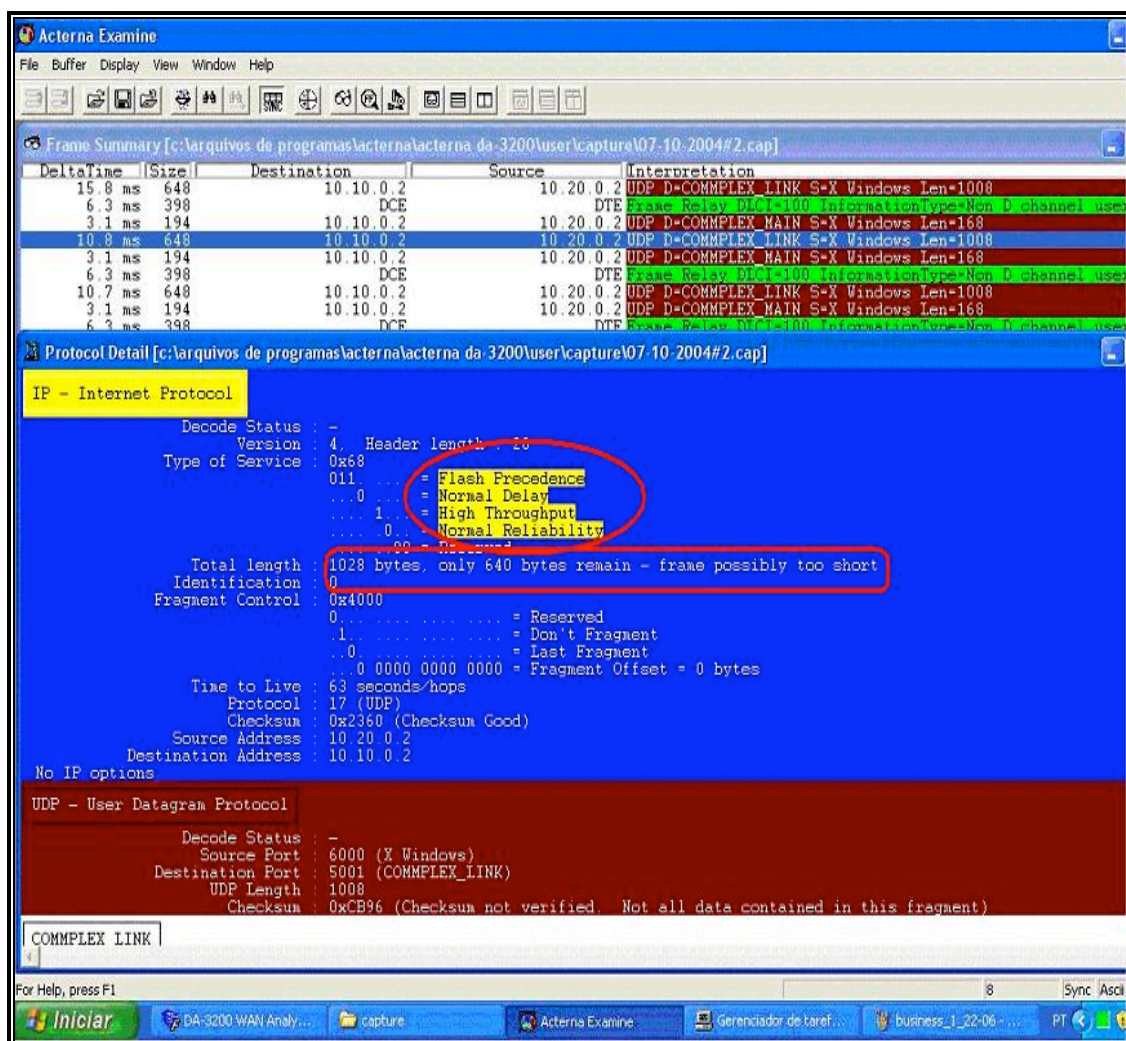


Figura 52 - Detalhes do fluxo classe business_1 de 2 a nível de protocolos IP e UDP.

Os detalhes destacados em círculos vermelhos (Figura 52) mostram que realmente a implementação de QoS e fragmentação surtiram efeito, cenário diferente do caso das medições sem LFI habilitada.

DeltaTime	Size	Destination	Source	Interpretation
6.3 ms	398	DCE	DTE	Frame Relay DLCI=100 InformationTyp
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Ler
10.8 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Ler
3.1 ms	194	10.10.0.2	10.20.0.2	UDP D=COMPLEX MAIN S=X Windows Ler
6.3 ms	398	DCE	DTE	Frame Relay DLCI=100 InformationTyp
10.7 ms	648	10.10.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Ler

Protocol Detail [c:\arquivos de programas\acterna\acterna da-3200\user\capture\07-10-2004#2.cap]	
Frame Relay - LAPF Link Access Procedure for Frame Bearer Services	
Decode Status	-
Frame Length	398
DTE-DCE	->
Destination	DCE
Source	DTE
Address Field	18 41
0001 10... 0100	= DLCI = 100 (Non D channel user information)
.... 0... ..	= Response
.... 0... ..	= No Forward Explicit Congestion
.... 0... ..	= No Backward Explicit Congestion
.... 0... ..	= Not Eligible for Discard
.... 0... ..	= Address Field Extension Bits
--- Fragmented Protocols over Frame Relay ---	
Control Field	0x03
000... 00...	= Modifier Function Bits
... 0... ..	= P/F
... 11...	= U Format
NLPID	0xB1 (FRF 12)
Fragment Header	0x4093
0... ..	= B = Off
... 1... ..	= E = On
... 0... ..	= C = Off
... 0... ..	= Fragment bit = 0
... 0 000... 1001 0011	= Sequence Number = 147
[Packet reassembly is currently disabled Fragmented frames for some protocols may decode incorrectly.]	
--- Multiprotocol over Frame Relay ---	
Control Field	00 00
0000 000... ..	= N(S) = 0
0	= I Format

Figura 53 -Fragmento 2 da classe business

A figura 53 representa uma das telas que representam os detalhes do segundo fragmento da classe business. Pois datagrama foi dividido em dois fragmentos - um fragmento UDP e o outro fragmento Frame Relay – pois, a fragmentação foi habilitada no acesso frame relay. O tráfego foi gerado pelo gerador MGEN, apesar de ser coletado pelo analisador acterna.

As diferenças básicas entre as telas da Figura 53 e as telas da Figura 51 - do primeiro fragmento de dados são: Protocolo - Frame Relay DTE e DCE para origem e destino respectivamente, tamanho de fragmento de 398bytes com variação de delay de 6,3ms. Percebe-se nessa figura o tamanho do segundo fragmento de 398bytes e o número de sequência 147, pois segue na ordem crescente, já que o primeiro fragmento tinha como número de sequência o número 146. As demais telas são idênticas às da figura imediatamente acima.

10.3.2 Tela ilustrativa da Medição Sem QoS e Sem LFI G726 e Sem cRTP

A Figura 54 é um exemplo ilustrativo da não LFI (*Link Fragmentation and Interleaving*), ou seja, não ocorreu a intercalação dos quadros de voz entre os pacotes de dados. Ademais, o pacote de dados não foi fragmentado.

Frame Relay	Size	Destination	Source	Interpretation
81.4 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1945 Timestamp=1644676065 SSRC=0x0F5C0006
1.1 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1946 Timestamp=1644676225 SSRC=0x0F5C0006
1.1 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1947 Timestamp=1644676385 SSRC=0x0F5C0006
1.1 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1948 Timestamp=1644676545 SSRC=0x0F5C0006
1.1 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1949 Timestamp=1644676705 SSRC=0x0F5C0006
6.1 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1950 Timestamp=1644676865 SSRC=0x0F5C0006
20.4 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1951 Timestamp=1644677025 SSRC=0x0F5C0006
20.2 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1952 Timestamp=1644677185 SSRC=0x0F5C0006
20.4 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1953 Timestamp=1644677345 SSRC=0x0F5C0006
20.1 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1954 Timestamp=1644677505 SSRC=0x0F5C0006
16.6 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=2086 Timestamp=11200 SSRC=0x0F930006
1.5 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1955 Timestamp=1644677665 SSRC=0x0F5C0006
14.7 ms	1034	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
2.8 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1956 Timestamp=1644677825 SSRC=0x0F5C0006
37.0 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1957 Timestamp=1644677985 SSRC=0x0F5C0006
3.5 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1958 Timestamp=1644678145 SSRC=0x0F5C0006
20.0 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1959 Timestamp=1644678305 SSRC=0x0F5C0006
20.0 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1960 Timestamp=1644678465 SSRC=0x0F5C0006
28.4 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=2087 Timestamp=11360 SSRC=0x0F930006
16.2 ms	1034	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
1.3 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1961 Timestamp=1644678625 SSRC=0x0F5C0006
1.1 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1962 Timestamp=1644678785 SSRC=0x0F5C0006
14.0 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1963 Timestamp=1644678945 SSRC=0x0F5C0006
23.5 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1964 Timestamp=1644679105 SSRC=0x0F5C0006
17.0 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1965 Timestamp=1644679265 SSRC=0x0F5C0006
50.8 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=2088 Timestamp=11520 SSRC=0x0F930006
16.2 ms	1034	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
1.4 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1966 Timestamp=1644679425 SSRC=0x0F5C0006
1.1 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1967 Timestamp=1644679585 SSRC=0x0F5C0006
1.1 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1968 Timestamp=1644679745 SSRC=0x0F5C0006
7.8 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1969 Timestamp=1644679905 SSRC=0x0F5C0006
96.5 ms	66	192.168.0.10	192.168.0.6	RTP G.729 Audio Seq=2089 Timestamp=11680 SSRC=0x0F930006
16.2 ms	1034	10.30.0.2	10.20.0.2	UDP D=COMPLEX LINK S=X Windows Len=1008
1.4 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1970 Timestamp=1644680065 SSRC=0x0F5C0006
1.1 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1971 Timestamp=1644680225 SSRC=0x0F5C0006
1.1 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1972 Timestamp=1644680385 SSRC=0x0F5C0006
1.1 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1973 Timestamp=1644680545 SSRC=0x0F5C0006
3.9 ms	266	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1974 Timestamp=1644680705 SSRC=0x0F5C0006
1.1 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1975 Timestamp=1644680865 SSRC=0x0F5C0006
1.1 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1976 Timestamp=1644681025 SSRC=0x0F5C0006
16.2 ms	66	192.168.0.5	192.168.0.10	RTP G.729 Audio Seq=1977 Timestamp=1644681185 SSRC=0x0F5C0006

Figura 54 - Detalhamentos adicionais sobre a Medição Sem QoS e Sem LFI G729 e Sem cRTP

Da Figura 54, constam os detalhes correspondentes a alguns protocolos separados por “abas” tais como Frame Relay, IP, UDP e RTP, advindo do Acterna. Constam, igualmente, dessa figura detalhes do Frame Relay como *DeltaTime* em ms correspondendo à variação do retardo; *Size* expresso em bytes correspondendo ao tamanho do quadro; *Destination* referindo-se ao destino do quadro transmitido; *Source* que diz respeito a fonte/origem do quadro transmitido, bem como o resultado de interpretação de cada quadro *frame relay* informando o tipo de protocolo de transporte utilizado -RTP, que transporta, por sua vez, em seu cabeçalho o tipo de codec utilizado (G.729), número de sequência dos frames e a numeração da sequência equivalente ao *Timestamp* dos quadros e o **SSRC**. Neste caso específico o protocolo RTP refere-se aos quadros de voz devido a conversação através de ramais de telefones e, os protocolos UDP, são os pacotes de dados *ftp* gerados a partir do gerador de tráfego MGEN. A ocupação da banda foi de 449.6kbps segundo a Tabela 40 a seguir.

```
#G729
Output queue: high size/max/dropped 0/256/0
Output queue: 0/128 (size/max)
30 second input rate 449600 bits/sec, 50 packets/sec
```

Tabela 40 - Ocupação da Banda da medição Sem QoS, Sem cRTP, sem LFI, codec G729.

A Tabela 40 representa um exemplo dos resultados da ocupação da banda registrado através das interfaces de saída dos roteadores para os testes realizados usando diferentes tipos de codec.

10.3.2.1 – Análise de QoS - configuração de protocolo em termos dos protocolos da rede.

Nos testes em que foram feitas medições Sem QoS e Sem LFI G729 e Sem cRTP, como já era de se esperar não seria possível ter uma aplicação de tempo real boa; então, o teste prático, cujos resultados estão evidenciados na figura acima comprovou que, realmente, era impossível tal prática, apesar de não termos ocupado toda a banda disponível, dado que o pacote ftp foi de 1000bytes contra os 66 bytes de fluxo de voz. Percebe-se durante o teste realizado, num intervalo de tempo de 2 (dois) minutos que a ligação telefônica tornou-se impraticável, devido aos ruídos intensos e falhas de segmentação dos fluxos de voz de forma aguda, causadas pelos altos valores de delay na serialização dos pacotes na interface da rede, que, por sua vez, foram causados pela não fragmentação dos pacotes de dados que foram, por outro lado, processados a uma alta taxa por segundo (50pps). Esses pacotes não fragmentados, todavia, causam a elevação do jitter na serialização dos quadros de voz que deviam ser serializados com um delay aproximado de, no máximo, 10ms somando aos 10 ms de intervalo entre a recepção e o envio de um novo quadro de voz. É especialmente recomendável que os pacotes cheguem em intervalos de tempo, constantes, de no máximo 20ms. Não deve haver variação de atraso que comprometa esses valores, pois na Figura 54 percebe-se que os valores de tempos do jitter superaram o recomendado e todas as demais estatísticas de medição referentes a esses testes, sobretudo, como se pode perceber, acabou originando instabilidades quanto a esse parâmetro. Com base nas evidências constantes da Figura 54 foi gerada a ilustração representada pela Figura 55 a seguir onde são apresentadas as informações referentes ao protocolo IP para o pacote de dados FTP.

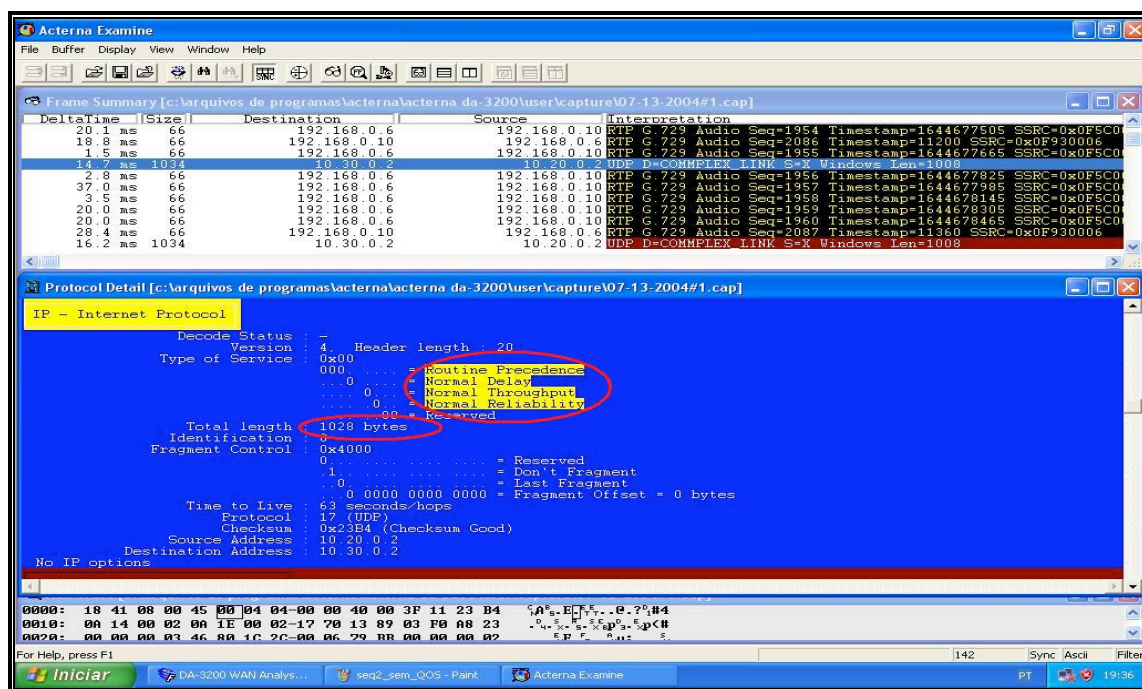


Figura 55 - Trecho ilustrando parâmetros de QoS para dados em Tráfego híbrido Sem QoS

Na Figura 55 - destacam-se, portanto, em “círculo de cor vermelha” os detalhes do fluxo, referenciando a não implementação de LFI e, por conseguinte, não será possível realizar a fragmentação. A Figura 55 é proveniente da Figura 54 anterior, onde foi tomado como referência um fluxo de pacote de dados para observar os detalhes dos protocolos e das configurações. Conforme delimitados em círculos vermelhos, pudemos perceber dos detalhes ajustados para o tipo de protocolo IP, como sendo *delay*, *throughput*, *Reliability* todos setados como normais e bit de fragmentação setado como 1 (um) LFI desabilitado, tipo de protocolo de transporte utilizado –UDP entre outros detalhes.

11 - CAPÍTULO XI – ANEXOS

**“Fortaleça-se com o positivo e não se deixe abater pelo negativo”
- DALE CARNEGIE**

Este capítulo assim como o capítulo - X (Apêndices) trata-se de um outro complemento aos demais onde será introduzidos alguns conceitos teóricos sobre as tecnologia MPLS, VPN, IP, pois a tecnologia do núcleo da rede da Operadora de Telecomunicações (OP) é IP/VPN/MPLS.

11.1 – ESTUDOS CONCEITUAIS SOBRE IP VPN/MPLS

Este capítulo em especial fala sobre alguns conceitos teóricos que servem de embasamento para os estudos práticos e também para o bom entendimento e contextualização dos assuntos propostos e que se enquadram dentro da realidade do laboratório disponibilizado. Assim este capítulo que é também formado por vários subcapítulos fala sobre alguns conceitos das tecnologias baseados nos protocolos IP/VPN/MPLS, pois, assim é definida a nuvem backbone da OP. Os serviços backbone são oferecidos na seguinte ordem metodológica:

11.2 - TECNOLOGIA MPLS (*Multiprotocol Label Switching*)

A rede disponibilizada pela OP para efeito de testes é denominada de *MiniRRede* CRT-UFF que envolve basicamente o núcleo da rede a tecnologia IP/VPN/MPLS *Multicasting*. Esta Mini-Rede faz parte de uma rede compartilhada, multifornecedor e multiplataforma. Esta possui tecnologia de enlace Frame Relay (com recomendação FRF.12) nos roteadores de acesso (CPE) - interface serial de 512Kbps que se conectam ao Backbone IP/VPN/MPLS, por onde passam os tráfegos da rede da OP, inclusive os tráfegos gerados na Mini-Rede UFF.

Durante os testes, foram focadas análises sobre a recomendação FRF. 12. Entretanto, como o núcleo da rede é coberto de forma transparente com a tecnologia MPLS, alguns testes nomeadamente os de cRTP foram analisados no domínio MPLS. Todavia não faz sentido realizar estes testes em backbones MPLS, uma vez que o backbone MPLS não costuma ter limitações da banda, ou seja, o anel MPLS tem a

banda disponível na ordem de dezenas a centenas de GigaBits por segundos (Gbps). É o caso da nuvem MPLS do backbone da OP que oferece links para serviços *multicating e multifornecedor* específicos a determinados clientes que são alimentados por uma determinada tecnologia de acesso.

A nuvem MPLS do OP agrega no seu acesso várias outras tecnologias de acesso como o Frame Relay, ATM (*Asynchronous Transfer Mode*), ADSL (*Asymmetric Digital Subscriber Lei*), Fibra Óptica, entre outras tecnologias de acesso [66]. Por essa razão, o Frame Relay, foi a tecnologia de acesso usada com maior incidência nos testes, pois o nosso cliente alvo deve ser alimentado por este acesso tecnológico[101]. O Frame relay está pendurado ao MPLS ponto-a-ponto, oferecendo serviços de voz, dados e IPTV (*Internet Protocol Television*) a alguns clientes da OP que havia na época.

O link de enlace que representa o caminho entre os CPEs (equipamentos de acesso aos clientes) e os PEs (equipamentos de Borda de backbone MPLS) é de 512kbps. Ainda nesta nuvem MPLS ficam pré-configurados todos os mecanismos de gerência da rede, bem como a configuração das rotas, regras e configuração de roteamento de tráfegos, implementação e configuração da Engenharia de tráfego [100]. É também através do backbone MPLS da OP que estão configurados as conexões intra-redes e inter-dominios, estes dando acesso às redes de outras operadoras e às conexões internacionais. Por este motivo, justifica-se uma breve introdução as tecnologias IP/VPN/MPLS enfatizando a sua adequação aos testes a que se propõe realizar.

11.2.1 - Algumas considerações importantes sobre as redes MPLS

As tecnologias MPLS são atualmente implementadas nas nuvens dos modernos *Backbones* das redes de telefonia e dados das operadoras de serviços e telecomunicações, agregando e dando suporte às demais tecnologias nos nós de acesso. As redes MPLS são assim dotadas, por exemplo, de mecanismos de encaminhamento de pacotes, que reúnem técnicas de transmissão orientadas para conexão e protocolos de roteamento para simplificar o processamento dos pacotes nos roteadores que ficam no caminho entre a origem e o destino [57].

Estes *Backbones* de Redes de Telecomunicações normalmente são baseados em tecnologia MPLS permitindo nos dias de hoje a convergência tecnológica de redes tradicionais de voz e dados com redes IP. Torna-se assim particularmente interessante a tecnologia MPLS, uma vez que ela prevê e provê inúmeras vantagens para a Engenharia de tráfego, além da facilidade oferece, permitindo agregar de forma transparente, muitas outras tecnologias de acesso ao núcleo da rede MPLS.

Essa transparência caracteriza-se pela sua facilidade de convergência e interoperabilidade com as diversas tecnologias de acesso hoje disponível no mercado para enfim, atender as demandas atuais da sociedade. O IETF (*Internet Engineering Task Force*) - órgão que desenvolveu o MPLS - pretendia com isso propor, inicialmente, um *upgrade* à implementação da tecnologia conhecida como *Label Based Switching* – LBS. Essa implementação, para além de outros objetivos e facilidades, surge num momento oportuno dando vida e agregando funcionalidades aos protocolos como, por exemplo, o IP e ATM, que se caminhavam rumo ao esquecimento [101].

Em termos conceituais entende-se, basicamente, que a MPLS enquanto uma tecnologia para protocolo de telecomunicações reside principalmente em funções que lhe são peculiares e inerentes, que a diferem de outras tecnologias que antes usavam protocolos puramente como o IP entre outros. Essa tecnologia **caracteriza-se na adição de rótulos (“labels”) aos pacotes IP, de forma a proporcionar regra e prioridade no encaminhamento (“routing”) dos pacotes em um Backbone IP** [77],[100]. Proporciona, igualmente, o encaminhamento e a comutação eficiente de fluxos de tráfego através da rede, funcionalidade esta que não está presente nos mecanismos de roteamento puro das então redes IP comuns. Assim em uma rede MPLS as informações são processadas e divididas em classes de serviços e os dados são encaminhados através de rotas estabelecidas anteriormente por essas classes, sendo feita apenas a comutação [44].

Há outras qualidades fundamentais inerentes a uma Rede MPLS como por exemplo o fato dela poder ser usada para tráfegos de múltiplos túneis através do núcleo da rede. Tunelamento é uma poderosa ferramenta intrínseca a esta tecnologia, uma vez que apenas os roteadores de *Ingress* e *Egress* daquele VPN - Túnel precisa entender o

‘contexto’ do tráfego subjacente transportado pelo respectivo túnel. Os conteúdos dos pacotes MLPS encapsulados aos túneis são transparentes aos roteadores nos núcleos da rede.

A Engenharia de Tráfego (ET) em redes MPLS permite definir dinamicamente rotas através de roteamento otimizado e criar rotas específicas para alguns fluxos de pacotes, permitindo ainda através de roteamento explícito criar caminhos preferenciais [80]. Com o roteamento explícito cria-se a possibilidade de classificação dos pacotes em classes de equivalência. A integração da infra-estrutura MPLS com as tecnologias emergentes de aprovisionamento de CoS (*Class of Service*) possibilita a escolha de caminhos mais adequados ao tráfego sensível a QoS, atribuídos a estas classes de equivalência.

Além disso, o roteamento explícito implementa o conceito de orientação à conexão, com emulação de circuitos virtuais mesmo em redes tipicamente não orientadas a conexão, como é o caso das redes IP. Assim se abre a possibilidade de suporte a serviços de priorização e reserva de recursos, como o *IntServ*.

Com o uso desta plataforma de QoS se propõe atingir os seguintes objetivos gerais [48]:

- ✓ Escalabilidade em preço e desempenho para toda a rede.
- ✓ Independência da camada de enlace (ATM, Ethernet, etc.);
- ✓ Independência da camada de rede. O foco principal dos trabalhos atuais é o IP, mas pode operar com redes IPX (*Internetwork Packet Exchange*), *DECnet* (*Digital Equipment Corporation network protocols*), etc.
- ✓ Coexistência com redes ATM nativas e esquemas de roteamento convencionais.
- ✓ Facilidade de suporte a redes multisserviço (dados, voz e vídeo) e capacidade de tratar diferentemente tráfegos de Melhor Esforço e Tráfegos sensíveis a QoS.

11.2.2 - Terminologia MPLS.

Esta subsecção traz definições sucintas sobre a principal terminologia utilizada na tecnologia MPLS para a Engenharia de tráfego na internet, os rótulos MPLS,

apresentando, portanto, o seu formato e a posição onde o mesmo é inserido no pacote IP.

11.2.3 - Label – (Etiqueta ou Rótulo)

O rótulo MPLS define, em parte, toda a terminologia da tecnologia MPLS numa comunicação entre os nós da rede do núcleo ao acesso. A etiqueta utilizada no MPLS tem tamanho fixo (4 bytes formado o cabeçalho MPLS) e curto e é utilizada como índice na tabela de encaminhamento (RFC 3031 [57]). Um *label* não é diretamente codificado com qualquer informação sobre os cabeçalhos do nível de rede, como por exemplo, endereços da fonte e do destino inicialmente não têm uma estrutura interna [74]. Ela é agregada ao pacote IP na entrada deste no domínio MPLS e retirada quando este deixa o domínio. A Figura 56 a seguir **Error! Reference source not found.**, representa o formato puro do mesmo.

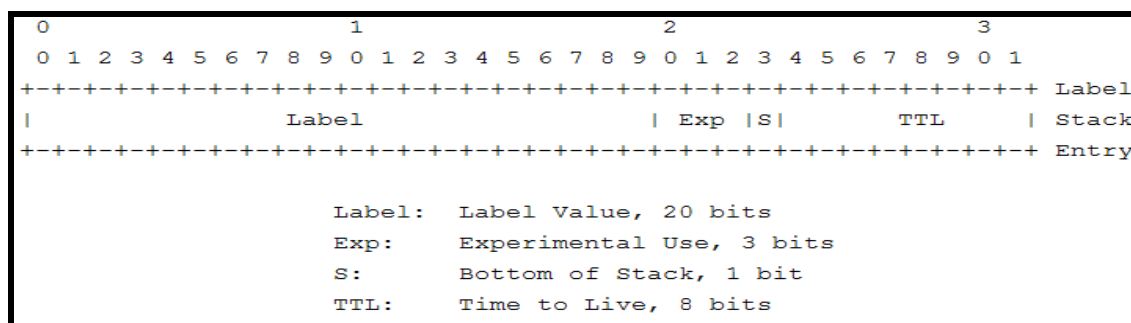


Figura 56- Formato do Label MPLS [61]

A Figura 56, apresenta uma visão técnica sobre o formato da etiqueta MPLS e a posição onde a mesma é inserida no pacote IP, pois, de acordo com o RFC 3032, os registros da pilha do rótulo aparecem depois dos dados dos cabeçalhos de camada de enlace, mas antes de quaisquer cabeçalhos da camada de rede [61], [44].

A Figura 57 a seguir representa esquematicamente o cabeçalho MPLS genérico com quatro campos, sendo o mais importante o campo Label que contém o índice para uma tabela de encaminhamento [44],[81].

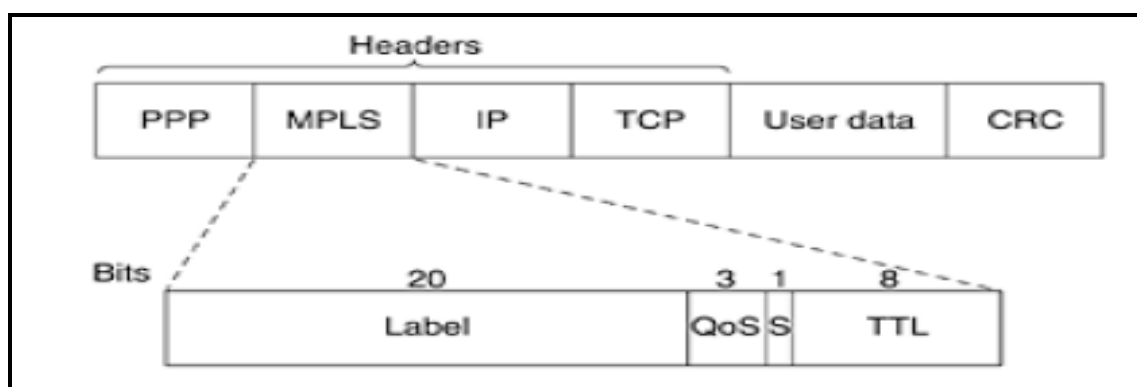


Figura 57 - Posição do cabeçalho MPLS no envio de segmento TCP com IP, PPP²⁵ [61]

Os campos que formam uma etiqueta completa para o cabeçalho - Label MPLS com um tamanho total de 32bits – são definidos pelos campos abaixo discriminados e os respectivos tamanhos em bits: - Etiqueta (*Label*) 20; - *CoS* (Exp) 3; - *Stack* (S) 1; - TTL 8.

Descrições dos campos do rótulo [61],[86].

- ✓ O campo etiqueta representa a etiqueta propriamente dita.
- ✓ O campo Exp (CoS) define a classe de serviço a que um pacote pertence, de onde se obtém informações dos parâmetros de garantia de QoS do pacote. Este campo é todavia de uso experimental e tem sido utilizado para classificar os pacotes em Classes de Serviços.
- ✓ Já o campo S (*stack*) suporta o enfileiramento de *labels* caso o pacote receba mais de um label concorrentemente. Este bit é setado para o valor um (1) para o último registro de entrada na pilha de etiqueta e zero (0) para todos os outros registros de entradas de pilha de etiqueta, conforme mostra a Figura 58 a seguir:
- ✓ O campo TTL (*Time to Live*) tem o mesmo papel que no cabeçalho IP, contar por quantos roteadores o pacote passou, num total de 255 saltos. Funciona tipicamente igual ao IP tradicional. No caso do pacote passar por mais de 255 roteadores, ele é descartado para evitar possíveis formação de loops [102].

25

O Campo PPP, surge com o advento de troca de rótulos no MPLS, com o intuito de solucionar o problema de onde pôr os rótulos já que os pacotes IP não foram projetados para circuitos virtuais. Não existia assim um campo disponível para números de circuitos virtuais dentro do cabeçalho IP. Por essa razão, adicionou-se um novo cabeçalho MPLS antes do cabeçalho IP. Em uma linha de roteador para roteador e usando-se o PPP como protocolo de enquadramento, das etiquetas trocas [81].

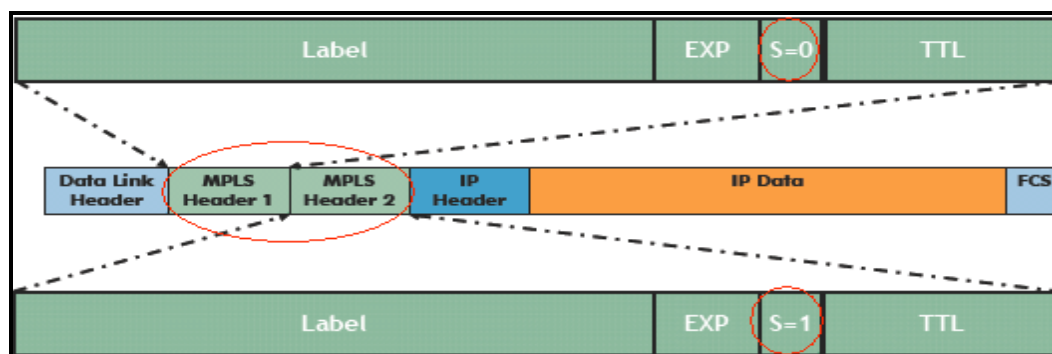


Figura 58 - Enfileiramento de cabeçalhos MPLS em um pacote de dados [85]

As redes MPLS precisam de um protocolo de distribuição de *Labels*, ou seja, um LDP, para a construção dos LSPs - [94],[103]. De entre os LDPs podemos citar:

- LDP - Foi o primeiro a ser desenvolvido, é prático e simples;
- RSVP-TE (*Resource Reservation Protocol-Traffic Engineering*), *FRR*, *loose LSPs*, etc, não falta funcionalidade.

O LDP define quatro tipos de mensagens que podem ser trocadas entre LSRs (*Label Switch Router*) parceiros:

- *Discovery Messages* (Mensagens de Descobrimento): Anuncia e mantém a presença de um LSR na rede
- *Session Messages* (Mensagens de Sessão): Estabelece, mantém e termina sessões entre parceiros LDP.
- *Advertisement Messages* (Mensagens de Anúncio): Cria, altera e finaliza mapeamento de etiquetas para FECs.
- *Notification Messages* (Mensagens de Notificação): Provê informação consultiva e sinaliza informações com erro.

NOTA:

O protocolo MPLS surge como uma arquitetura emergente que, através do modelo de encaminhamento de pacotes baseados em *labels*, permite a interoperabilidade e compatibilidade de diversas tecnologias de rede usadas pelos principais *backbones* do mundo. Pode-se ainda citar outras características importantes propostas por esse protocolo:

- ✓ A agilidade no encaminhamento de pacotes proporcionada pela simplificação no processo de roteamento, onde os pacotes são analisados apenas nas bordas de um domínio MPLS e são somente comutados pelos demais roteadores;
- ✓ A implementação de orientação a conexão em redes IP, propicia a engenharia de tráfego;

- ✓ O suporte ao IP QoS, possibilita a utilização de QoS em redes baseadas em IP.

Isto tudo sem alterar totalmente a estrutura já existente das redes de comunicações.

Todas essas características nos levam a acreditar no protocolo MPLS como uma tecnologia capaz de melhorar sensivelmente a qualidade das transmissões de voz e vídeo (através da QoS), a segurança (através das VPNs) e a velocidade e planejamento nas transmissões de dados (através do TE - *Traffic Engineering*).

11.2.4 – MPLS – e os mecanismos de encaminhamento dos pacotes.

O mecanismo de encaminhamento de pacotes em redes MPLS é baseado em *labels*. Os pacotes que chegam dentro da rede têm um ou mais cabeçalhos MPLS aplicados nos LER ²⁶(*Label Edge Router*) *Ingress*. O LER *Ingress* identifica o LER *Egress* para que pacotes devem ser enviados e os correspondentes LSP (*Label Switch Path*). No mecanismo de encaminhamento de *Labels* MPLS, costuma ser enviado um ou mais cabeçalhos, isto porque, os LER's em uma rede particular poderá ser envolvido em múltiplos serviços L3 VPN, L2VPN, VPLS (*Virtual Private LAN Services*).

Em uma rede MPLS um pacote que a percorre está condicionado, necessariamente, a três estágios diferentes: Estagio primeiro: ele sofre uma transição do seu nível de encaminhamento L3 que ocorre nos roteadores de borda, para encaminhamento em rotulados MPLS, conhecidos como processo de adição de um *label* MPLS ao cabeçalho do pacote IP que ocorre no núcleo da rede. Como o estágio segundo, um pacote já com *Label* ganha condições para atravessar um caminho MPLS. O mecanismo que garante esta condição e que conhece todos os pacotes que atravessam a rede é denominado de caminho – LSP (*Label Switched Path*).

O LSP é assim um caminho configurado anteriormente ao encaminhamento de qualquer pacote que lhe dá suporte em todo o trajeto, sendo este caminho orientado a conexão. Já no ultimo estagio, o terceiro, o pacote volta ao encaminhamento de nível três do outro lado do destino garantindo assim a formação do processo de remoção do

26

Atua como fronteira entre o encaminhamento de nível três e o encaminhamento MPLS, adicionando um rótulo a um pacote não rotulado, e remover os rótulos de um pacote rotulado. Um LER que adiciona um rótulo a um pacote é chamado de LER *ingress* e um LER que remove o rótulo de um pacote é chamado de LER de *egress*.

label do cabeçalho do pacote e envia-o ao protocolo de nível três apropriado para outros tratamentos finais. O processo de encaminhamento de um pacote rotulado ou com *label* MPLS é normalmente chamado de chaveamento ou troca de rótulo (*Label Switching*), pois às vezes o valor do rótulo pode mudar a cada passo do LSP. Entretanto, o mecanismo da rede capaz de encaminhar um pacote rotulado é chamado de LSR (*Label Switch Router*) [80].

11.2.5 - MPLS e o seu nível de agregação dos fluxos

O MPLS possui uma característica peculiar que é a forma como permite níveis de agregação dos fluxos, agregando vários fluxos. É comum ter o seu próprio conjunto de rótulos na sub-rede. Porém, é mais comum os roteadores agruparem vários fluxos que terminam em certo roteador ou LAN (*Local area network*) e usarem um único rótulo para eles. Estes fluxos agrupados sob o um único rótulo pertencem a mesma FEC (*Forwarding Equivalence Class*)[81]. Essa classe abrange não apenas os lugares para onde os pacotes estão indo, mas também sua classe de serviço, porque todos os seus pacotes são tratados do mesmo modo para fins de encaminhamento [57]. Dentro do domínio MPLS os pacotes IP podem ser encaminhados de duas maneiras: *hop-by-hop*, que se traduz no encaminhamento normal do IP ou baseado nos “*labels*” (etiquetas ou rótulos) agregados aos pacotes, utilizando o conceito de circuito virtual comutado. Nesta última forma o RFC 3031 destacam-se os principais benefícios para uma rede MPLS conforme segue [57],[48]:

- ✓ **Roteamento Simplificado:** O encaminhamento dos pacotes é feito baseado em *labels* curtos e de tamanho fixo que são agregados aos pacotes na entrada do domínio MPLS. Isto permite que os pacotes possam ser agrupados em FECs (*Forwarding Equivalence Class*) num processo conhecido como roteamento explícito efetuado pelos nós principais da infraestrutura MPLS, denominados LSR (*Label Switching Routers*). Esse agrupamento de pacotes em FEC se dá de acordo com a informação contida no referido *label*.
- ✓ **Roteamento Explícito Eficiente:** o MPLS permite que os pacotes sejam classificados a partir de *labels* atribuídos na admissão dos nós MPLS e encaminhados, dentro de uma mesma classe, num caminho virtual sem a necessidade de ser analisado nó a nó. Esta técnica (semilar a técnica utilizada pela ATM (*Asynchronous Transfer Mode*)) permite que seja criado um caminho

virtual dentro do domínio para o encaminhamento dos pacotes evitando que estes sejam analisados em cada nó da rede permitindo melhor desembaraço no encaminhamento e recepção de pacote.

- ✓ **Suporte a Engenharia de Tráfego:** A habilidade em definir rota dinamicamente, plano de comprometimento de recurso baseado na demanda conhecida e otimização da utilização dos recursos de rede, tem sido referenciada como sendo Engenharia de Tráfego (TE). No MPLS é possível criar rotas específicas para fluxos de pacotes, cujo destino e origem sejam nós particulares na rede. Por outro lado, nas redes baseadas em *datagramas*²⁷, como as redes IP, a TE é dificultada, devido ao caráter de não orientação à conexão. Dentro deste enfoque, a arquitetura MPLS possibilita que fluxos de dados oriundos de um nó de entrada particular, direcionado para um nó de saída particular, possam ser identificados individualmente, como num circuito virtual. Ademais, com o roteamento explícito é possível criar caminhos preferenciais para fluxos de pacotes específicos (LSP – *Label Switched Path*).

Suporte a QoS: A capacidade do MPLS em estabelecer uma orientação à conexão (no estabelecimento dos LSPs) entre os nós de entrada e de saída preenche uma das principais lacunas das redes IP para implementação de Serviços Integrados. O advento das FECs e a possibilidade de associar estas classes de equivalência a classes de serviços também impulsionam a utilização desta arquitetura como suporte ao *DiffServ* do IETF. Baseado nos outros itens acima é possível garantir de forma explícita e confiável uma boa qualidade de serviço (QoS) no domínio MPLS.

O MPLS é, portanto, uma tecnologia utilizada em Backbones, e tem o objetivo de solucionar problemas atuais de redes de computadores. Dentre os problemas a lidar por esta tecnologia consta a velocidade, escalabilidade, gerenciamento de QoS e a necessidade de engenharia de tráfego – TE (*Traffic Engineering*), entre outros parâmetros.

11.2.6 – De entre algumas vantagens tecnológicas, constam:

- ✓ A possibilidade de substituição ou overlay de redes “legadas” como, por exemplo, a ATM, FR (Frame Relay), por equipamentos de nova geração

²⁷ **Datagrama:** Unidade de informação que a Camada de Transporte passa para a Camada de Rede

baseados em IP, mantendo o serviço ao cliente e o acesso final do ponto de presença da rede inalterados.

- ✓ Garantia de um tráfego diferenciado como Multimídias (voz, vídeo e dados) e aplicações críticas, com suporte e garantia de QoS, dividida em classes de serviço: **Multimídia**: priorização de tráfego dos pacotes multimídia (ex.: vídeoconferência); **Voz**: priorização de tráfego dos pacotes de voz (ex.: Interligação de PABX (*Private Automatic Branch eXchange*), telefonia IP); **Dados Expressos**: priorização de tráfego de dados de aplicações críticas; **Dados**: tráfego de dados sem priorização (*Best-Effort*²⁸).
- ✓ A introdução de serviços como VPN (*Virtual Private Network*) e Metro Ethernet, com a utilização compartilhada do core MPLS por diversos clientes / circuitos de forma segura e controlada.
- ✓ A criação de diferentes níveis de classes de serviço e engenharia de tráfego para a rede de serviços de nova geração MPLS, permitindo um nível de priorização de serviços e controle de qualidade em tempo real anteriormente não disponíveis em ambientes IP;
- ✓ As características de autocorreção inerentes aos protocolos de roteamento no core IP / MPLS permitem mudanças de configuração no envio de pacotes (reroteamento em função de falhas e métricas de QoS em tempo real) sem interrupção de serviço.
- ✓ Alocação de largura de banda em tempo real para uma chamada de vídeo em um ambiente celular baseado em IMS (*IP Multimedia Subsystem*) [45],[74];
- ✓ Permite reroteamento rápido – Fast Rerouting;
- ✓ Roteamento otimizado pelo caminho alternativo;
- ✓ Permite montar uma infra-estrutura de serviço IP VPN (*Virtual Private Network*), frequentemente denominada “*Layer 3 MPLS*” ou “ *BGP/ MPLS VPN*”. Esta aplicação é especificada na RFC 2547. [47]

A convergência dos serviços para uma única rede com core MPLS traz, assim, as seguintes vantagens [44],[42a]:

- Menor investimento;

²⁸ **Best-Effort (BE)** - Modo operação de entrega de dados utilizada pelo IP, onde a estrutura de transporte não assegura a entrega de serviço.

- Simplicidade operacional e provisionamento;
- Sem a limitação 4096 VLANs (*Virtual Local Area Network*);
- Restauração 50ms, não utilização do protocolo STP.
- Transmissão ótica otimizada para 10 Gbps nos barramentos de troncos e com 40 Gbps de velocidade agora disponibilizado como caso ótimo.

Com tudo isso, as redes baseadas em IP geram mais retorno dos investimentos, deixam habilitada outra solução para garantir novos serviços na rede.

11.2.7 - Funcionamento e transporte de dados MPLS sobre os nós de acesso.

O EoMPLS (*Ethernet over MPLS*) transporta todos os dados recebidos de uma determinada rede ethernet ou VLAN (*Virtual LAN*), suportando mapeamento para 802.1p para os bits de QoS do MPLS (*EXP Bits*), além de “*traffic shapping*”; já o ATM pode ser transportado de duas maneiras: AAL5 over MPLS e transporte de células transparentes.

Na primeira alternativa de transporte, os circuitos ATM terminam nos roteadores de borda, enquanto que na segunda as células são empacotadas em quadros MPLS sem qualquer manipulação, permitindo um transporte com melhor desempenho. Com relação ao *Frame Relay*, os PVCs terminam nos PEs e as informações de BECN, FECN DE e C/R são transmitidas no cabeçalho dos quadros MPLS. Esta última opção de AToM (*Any Transport over MPLS*) é indicada para o transporte de tráfego oriundo de comutadores Frame Relay ainda existentes dos pontos de presença (PoPs) da operadora [68]. Nas atuais implementações o roteador do provedor situado na borda da rede, também chamado de PE (*Provider Edge*), recebe o pacote IP e o encapsula em um pacote MPLS. Desse ponto em diante, a informação de roteamento é controlada pelo cabeçalho MPLS. Tendo o IP encapsulado em MPLS, a fim de se ter os benefícios de TE – *Traffic Engineering*, que foi projetado para rotear tendo em vista certas limitações na seleção de caminhos existentes nos protocolos de roteamento IP tradicionais, tais como o OSPF (*Open Shortest Path First*) ou IS-IS (*Intermediate System to Intermediate System Routing Exchange Protocol*) [66]. Estes protocolos levam em consideração o caminho mais curto entre a fonte e o destino, mas não consideram o tipo de pacote transmitido, por exemplo, voz (sensível à latência) e e-mail (insensível aos atrasos), capacidade dos links, condições de congestionamento da rede e políticas de balanceamento de carga.

Contrariamente a tudo isso, o TE, por outro lado, considera as condições de rede e os atributos do pacote IP na hora de determinar o melhor caminho para que o mesmo trafegue da fonte ao destino utilizando um circuito pré-determinado. Esta característica (automática) permite que as operadoras possam utilizar melhor a banda das suas redes e oferecer um serviço consistente e de alta qualidade aos usuários finais [44].

Conforme anteriormente descrito, a MPLS permite de forma sustentável criar e gerenciar logicamente redes separadas virtualmente que funcionam como se fossem redes fisicamente separadas. O CRT implementa a metodologia VPN (*Virtual Private Network*), da qual destacamos, no subcapítulo seguinte, algumas características das suas redes:

11.3 – VPN / MPLS

Uma VPN MPLS consiste em um conjunto de sites que são interligados por meio de uma rede - *Core Provider MPLS*. Apesar disso, é também possível aplicar políticas diferentes para diferentes sistemas que estão localizados no mesmo local. Em cada site existe pelo menos um CPEs ou várias, que são atribuídos a um ou mais PEs.

Os PEs usam o *Border Gateway Protocol - Multiprotocol* (MP-BGP) para dinamicamente se comunicar uns com os outros. Usando o MP-BGP, os PEs traduzem os endereços IPv4 em IPv4 VPN. O conjunto de endereços IP usados em uma VPN, deve, porém, ser exclusiva do conjunto de endereços usados na rede do provedor. Todo CE deve ser capaz de comunicar-se com os PEs aos quais está diretamente ligado. Dessa forma, os endereços IP dos PEs não devem ser repetidos em qualquer VPN [87][99].

O BGP (*Border Gateway Protocol*) é o protocolo usado para a comunicação entre os PEs, embora em um único SA (*Sistemas Autônomos*). Um dos protocolos de roteamento recomendado na Internet é o OSPF. Já entre SAs é necessário um protocolo diferente entre o BGP, porque os objetivos desses protocolos de gateway interior e exterior são distintos. Tudo o que um protocolo de gateway interior precisa de fazer é movimentar pacotes de forma mais eficiente possível, de origem até o destino. Ele não precisa de se preocupar com política [81].

Cada roteador BGP contém um módulo que examina e conta as rotas para um determinado destino, retornando um número que identifica a "distância" até esse destino em relação a cada rota.

Qualquer rota que viole uma restrição política recebe automaticamente uma contagem infinita. Estes roteadores de protocolos de gateway exterior têm de se preocupar muito com as políticas. O BGP é, no entanto, um protocolo fundamentalmente de vetor de distância (DV), mas é bem diferente da maioria dos outros, como o RIP (*Routing Information Protocol*). Em vez de manter apenas o custo para cada destino, cada roteador BGP tem o controle de que caminho está sendo usado. Da mesma forma, em vez de fornecer periodicamente a cada vizinho seu custo estimado para cada destino possível, o roteador BGP informa aos seus vizinhos o caminho exato que está sendo usando [99]

Os protocolos de gateway exterior em geral e o BGP em particular foram projetados para permitir a imposição de muitos tipos de políticas de roteamento no tráfego entre SAs. Em geral, as políticas envolvem considerações políticas, econômicas e de segurança. Vejamos alguns exemplos de restrições de roteamento [81]:

- Nenhum tráfego deve passar por certos SAs.
- Só passará pela Albânia se não houver nenhuma alternativa ao destino.
- O tráfego que começar ou terminar na IBM não deverá transitar pela Microsoft.

11.3.1 - Benefícios da VPN/MPLS para os serviços e fornecedores.

VPNs tem basicamente como benefícios [42a]:

- Segurança e privacidade iguais a *Frame Relay* ou ATM;
- Provisionamento simples, rápido, com operação transparente ao núcleo da rede;
- Formas variadas de acesso baseadas em tecnologias conhecidas (MPLS e BGP);
- Flexibilidade de endereçamento;

- Escalável para qualquer conectividade para intranets e extranets que englobam várias empresas;
- Pode ser usado em conjunto com QoS e Engenharia de Tráfego;
- Separação do Plano de Controle do Plano de Encaminhamento;
- Possibilidade de usar IP's não válidos;
- Segurança e Isolamento totais do tráfego em uma mesma rede;
- Aplicação de QoS para VPNs, integração com outros Backbones.

Com relação aos fornecedores de serviços, passo a citar os benefícios da VPNs MPLS que se seguem [87]:

- Uma plataforma para implantação rápida de novos serviços de valor agregado ao IP, incluindo intranets, extranets, voz, multimídia, etc;
- Privacidade e segurança iguais à VPNs Layer-2, restringindo a distribuição de rotas VPN somente para os roteadores que são membros dessa VPN, MPLS utilizados para o encaminhamento;
- Ótima integração com *intranets* cliente com maior escalabilidade a milhares de sites por VPN e centenas de milhares de VPNs por prestador de serviços;
- *Class of Service* (CoS) com suporte para múltiplas classes de serviço dentro de uma VPN, bem como as prioridades entre VPNs;
- Fácil adesão e gerenciamento de VPN com implantação rápida de novas VPNs;

11.3.2 – VPN - visão do cliente da rede

Uma análise da VPN a partir do ponto de vista do cliente, permite ver os seus roteadores internos a comunicar com os seus roteadores de borda de clientes (EC) a partir de um site para o outro, através de uma VPN gerenciado pelo prestador de serviço, conforme indica a Figura 59 a seguir. Essa visão é, portanto, sem dúvida uma das vantagens de se empregar VPNs:

Aos olhos do cliente seria como que se fosse uma comunicação direta com os seus sites a partir do provedor, isto é, como se tivessem sua própria rede privada,

embora o seu tráfego esteja atravessando uma infraestrutura da rede pública que eles estão compartilhando com outras empresas [87].

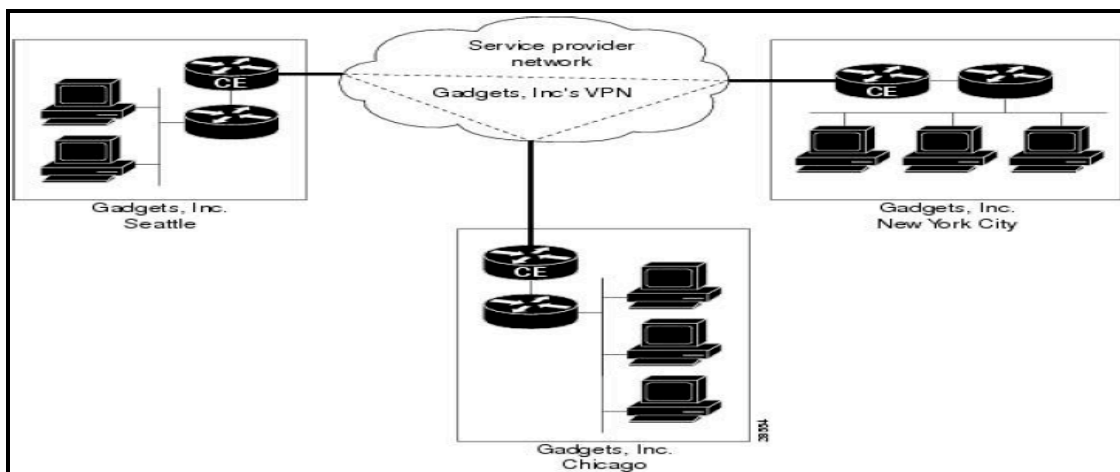


Figura 59 - VPN - visão do cliente da Rede [87]

11.3.3 – VPN – PE's a visão do provedor de serviços da rede

A conexão entre PE's e CE's costuma ser bastante simplificada e as rotas aprendidas pelo PE's serão redistribuídas dentro da VPN²⁹ via MP-BGP, podendo ou não ser usado um protocolo de roteamento entre PE-CE³⁰. Porém, as conexões típicas são via BGP, Rota estática ou OSPF; as demais conexões serão definidas caso a caso [47],[87].

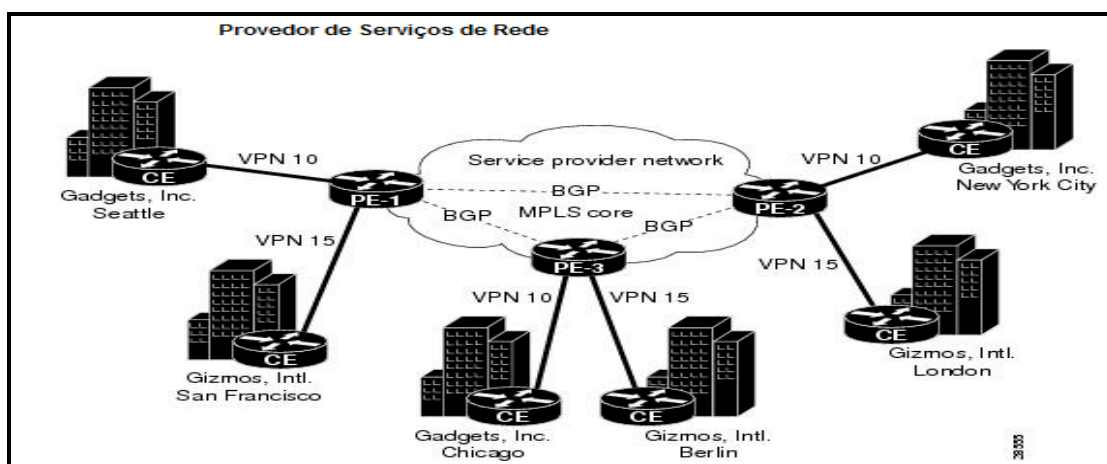


Figura 60 - VPN visão do provedor de serviços da rede [87]

Roteadores P (Provider)

São os equipamentos do núcleo da rede MPLS que interligam os PEs, são os responsáveis por transportar o tráfego entre as bordas da VPN/MPLS

Roteadores PE (Provider Edge - roteador de borda do provedor)

Interface da nuvem MPLS com o cliente. Ponto onde é iniciada a VPN.

Roteadores CE (Customer Edge - Equipamentos de Borda do cliente)

Equipamentos dos clientes que fazem interface com os equipamentos do provedor, PE.

Na borda da rede do fornecedor os roteadores são *Provider Edge* (PEs). Dentro da rede de fornecedor, roteadores de outros fornecedores sempre que necessário costumam ser designados como roteadores P que se comunicam uns com os outros e as PEs, através do *Border Gateway Protocol - Multiprotocol* (MP-BGP). Percebe-se, na Figura 60, que o prestador de serviços precisa de manter apenas as ligações VPN entre os PEs e EC.

PEs mantêm separadas as tabelas de roteamento chamadas roteamento de VPN e tabelas de encaminhamento (VRFs). O VRFs contém as rotas para sites relacionados apenas diretamente aos VPN's. As atualizações de troca dos endereços VPN-IPv4 e rótulos nos PE's dão-se através das sessões MP-iBGP.

11.3.4 - VPNs MPLS e as tabelas de encaminhamento (VRFs)

As VPNs MPLS são criadas em *Layer 3* e baseiam-se no modelo de pares, o que as tornam mais escaláveis e fáceis de construir e de gerenciar do que VPNs convencionais. Estas permitem agregar valores tipo hospedagem de dados, serviços de telefonia. Considera-se que o modelo MPLS VPN representa um fiel modelo *peer* VPN que impõe a separação de tráfego através de atribuição única de tabelas VPN, via encaminhamento (VRFs) para cada cliente VPN (vide a Figura 61 a seguir). Assim, os usuários de uma VPN específica não podem ver o tráfego fora do seu VPN.

A separação do tráfego VPN ocorre, entretanto, sem *tunneling* ou criptografia, porque é construída diretamente na rede. MPLS VPN oferece a possibilidade da informação de roteamento sobre uma VPN particular esteja presente apenas nos roteadores PE (constituem o *Backbone*) atribuídos a essa VPN. Devido a este pormenor, o tráfego é completamente isolado entre as VPNs [47],[87];

Esta rede utiliza várias tabelas de comutação, uma para cada VPN:

- Estas tabelas são chamadas VRF (*Virtual Routing and Forwarding*)

Possuem as rotas pertencentes à VPN:

- Rotas recebidas dos CEs diretamente conectados; Rotas recebidas dos PEs remotamente conectados via iBGP.

Um determinado conjunto de sites pode estar em uma ou mais VPNs.

A VPN pode consistir em sites (ou sistemas) que são todos da mesma empresa (*intranet*), ou empresas diferentes (*extranet*) que pode consistir de sites que todos são atribuídos ao mesmo serviço de provedor de *Backbone*, ou para *Backbones* prestador de serviço diferente [87].

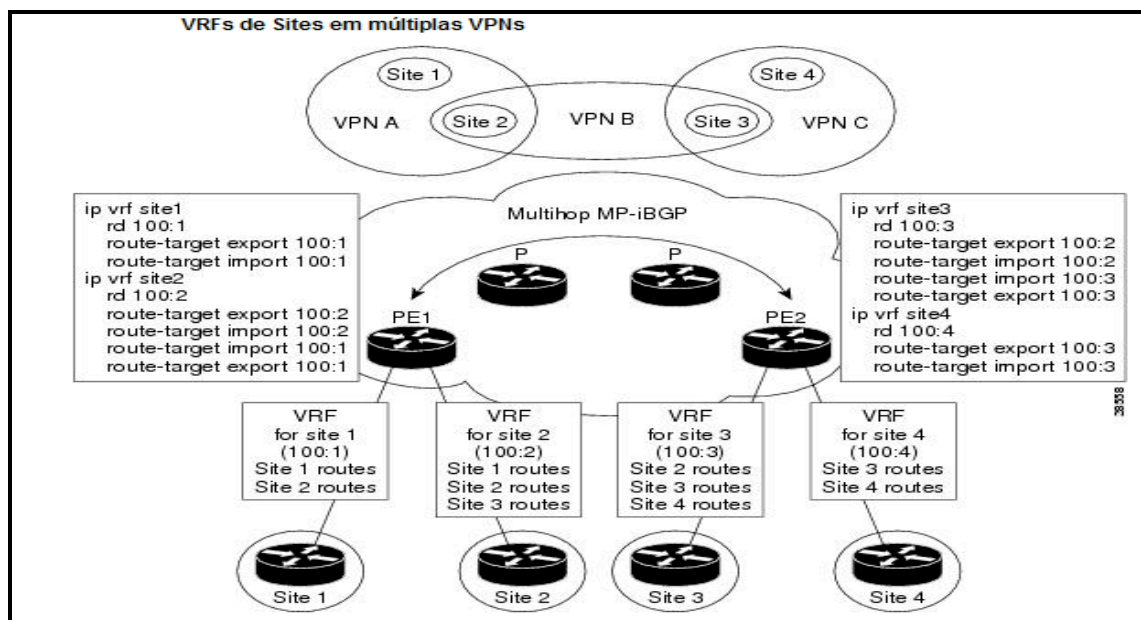


Figura 61 - VRF's de sites com múltiplas VPN em um core MPLS [87]

A tabela VPN de roteamento e encaminhamento (VRF³¹) é um elemento-chave na tecnologia VPN MPLS. Uma tabela VRF está normalmente associada aos seguintes elementos:

- Tabela de roteamento IP;
- Um conjunto de interfaces que usam a tabela derivada encaminhamento;
- Um conjunto de protocolos de roteamento e encaminhamentos pares que injetam informações na VRF.

Cada PE mantém, portanto, um ou mais VRFs. VRFs só existem nos PEs. A VRF é um exemplo da tabela de roteamento. Uma VPN pode conter um ou mais VRFs em uma VRF PE. Estas tabelas, conforme evidenciadas na figura 06 - acima contém a relação das rotas que devem estar disponíveis para um determinado conjunto de sites.

31

Para os equipamentos da plataforma Cisco, verificar que: As VRFs usam tecnologia CEF, pois a VPN deve ser habilitada para a CEF (*Cisco Express Forwarding*) e as VRF's são associadas também aos fluxos de tabela de encaminhamento, com base na tecnologia *Cisco Express Forwarding* (CEF).

As tabelas VRF em PE, conforme ilustra a Figura 61 acima, são utilizadas apenas para os pacotes que chegam a partir de um CE que está diretamente ligado ao dispositivo PE. Elas não são usados para roteamento de pacotes que chegam de outros roteadores que pertencem ao Backbone da operadora. Assim, como resultado, pode haver várias rotas diferentes para o mesmo sistema, em que a rota a ser seguida por um pacote é determinada pelo site de onde o pacote entra no *Backbone*. Assim, pode-se ter uma rota para uma rede de dados IP para os pacotes do *extranet* (onde o caminho leva a um *firewall*³²) e uma rota diferente para a mesma rede para pacotes a partir da *intranet*.

A rede IP constitui uma “arquitetura” base para qualquer outra rede de telecomunicações, pois o IP é o protocolo base que provê subsídio ao empilhamento dos demais protocolos das camadas acima do nível (*layer*) três (L3). Face ao exposto, a subseção seguinte apresenta uma breve contextualização do protocolo IP. Ademais, os testes da compressão do cabeçalho e fragmentação de pacotes incluem também, necessariamente, alguns conhecimentos teóricos sobre, por exemplo, o cabeçalho IP e suas características intrínsecas.

11.4 - Protocolo IP e os princípios de serviços em redes IP

O estudo e embasamento teóricos do protocolo IP são necessários uma vez que, durante os testes laboratoriais, os campos de cabeçalho IP são constantemente usados quando se refere à classificação dos pacotes, compressão do cabeçalho IP em frames de voz, nas metodologias de fragmentação a nível 3 (IP) e nas metodologias de fragmentação com intercalação de frame de tempo real que ocorre à nível 2 (Enlace Frame Relay).

A fragmentação a nível do IP é a técnica que ocorre, normalmente, no nível internet (L3) em que as redes executam-na quando os datagramas excedem a MTU - ethernet de 1500bytes. Dado o objetivo dessas medições, mostra-se necessário chegar ao problema em si, conforme sugere o título dessa dissertação. Para resolver o problema em si, uma das principais metodologias a adotar é a da necessidade de realizar a fragmentação com intercalação de quadros de voz entre os pacotes de dados, conforme o capítulo abaixo em

32

Firewall: Dispositivo de uma rede que permite aplicar política de segurança a um determinado ponto da rede, regulando o tráfego de dados entre redes distintas e impedindo a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra, protegendo assim os recursos de hardware e software.

que o assunto é tratado através das recomendações Frame Relay. Pelos expostos acima, torna-se conveniente tratar de forma sucinta algumas características do IP. O serviço de camada da rede é tipicamente denominado serviço de melhor esforço, isso porque o protocolo IP não garante que o pacote chegue dentro de determinado tempo ao destino nem que uma série de pacotes chegue na ordem correta. Na verdade, não garante ao menos que o pacote chegue ao destino [8]. Assim o IP fornece os serviços de datagrama não orientados a conexão.

O IP não especifica qual a tecnologia da rede a ser utilizada, de forma que o mesmo seja suportado, praticamente, por qualquer tipo de rede. Com o crescimento da Internet em capacidade e topologia, o protocolo IP, de fato, vem se tornando cada vez mais num padrão para as diversas aplicações, inclusive em *Backbones* de alta velocidade. O protocolo IP pode ser utilizado em redes tipicamente IP cliente – servidor e ou em redes de diversas tecnologias de alta velocidade diferentes, em especial às redes FDDI (*Fiber Distributed Data Interface*) e Fast/Gigabit Ethernet. Também está sendo estudada e padronizada a utilização do IP diretamente sobre redes ópticas, reduzindo o *overhead* das camadas intermediárias [8].

O IP foi projetado para o uso em larga variedade de links de transmissão, embora o tamanho máximo de um datagrama IP seja de 64kb. A maioria de links de transmissão força os pacotes a um limite menor que o tamanho máximo a cada pacote, chamado de MTU. Neste caso, um recurso usado pelo IP (e por vários outros protocolos) é o da fragmentação (segmentação) e remontagem. Neste processo, o roteador negocia com os periféricos da rede e com o próximo roteador o tamanho máximo que pode ser usado naquela sub-rede. *Datagramas* com tamanhos maiores devem, então, ser fragmentados.

A RFC-760 [43] e também a RFC-791 [71] descreve a operação do IP baseando em duas funções básicas: endereçamento e fragmentação. Os módulos de Internet (camada da Internet) usam os endereços da portadora contidos no cabeçalho inter-rede (Internet) para transmitir datagramas em direção aos seus destinos. A seleção de um caminho para transmissão é chamada de roteamento. A camada Internet usa campos no cabeçalho Internet para fragmentar e remontar os datagramas Internet quando necessários para transmissão de "pequenos pacotes" através da rede. O modelo de operação existente na camada de inter-rede consiste em que cada *host* (estação hospedeiro) tome e fique ocupado com parte de comunicação da camada da Internet e que cada *gateway* esteja interconectado a redes.

Estes módulos compartilham regras comuns para interpretar campos de endereço e também para fragmentar e remontar datagramas da camada IP. Além disso, esses módulos (especialmente em gateways) podem ter procedimentos para tomar decisões de roteamento e outras funções. O IP trata cada *datagrama* IP como uma entidade independente sem conexão para qualquer outro datagrama da camada Internet. Não existem conexões ou circuitos lógicos nem circuitos virtuais. O IP usa quatro mecanismos chaves para fornecer seu serviço: *Type of Service, Time to Live, Options, and Header Checksum*, conforme se pode notar na figura que se segue da subseção formato de datagrama IP. Nesta subseção, além dos campos chaves usados pelo IP para fornecer seus serviços, serão, igualmente, discutidos alguns dos outros campos inerentes ao datagrama IP,[RFC-760] [43].

11.4.1 - Formato do Datagrama IP

Um *datagrama* IP possui um total de 20 bytes de cabeçalho, além de outras informações como dados, opções, etc..., característica própria do protocolo IP que na sua quarta versão (IPv4), ou seja, a versão usada comercialmente nos dias de hoje, possui quatro octetos de 8 bits cada totalizando 32 bits de comprimento que serão corretamente divididos por cada campo de um datagrama IP “linha a linha” (32 bits). Datagrama é a denominação dos pacotes transportados pelo IP, ou seja, são pacotes de informação em um sistema de comutação de pacotes que contém seu endereço e rota / destino. Embora o IP vá já na sua sexta versão (IPv6) , a versão Pv4 ainda não perdeu o seu lugar devido a sua ampla aceitação e uso eficaz no mercado, inclusive, em pesquisas.O IPv6 desta forma não permite fragmentação nos roteadores [8]. A Figura 62 a seguir ilustra o formato do datagrama IPv4, seguido da descrição dos seus campos, segundo a recomendação: RFC-791 [71], [7] e também a RFC-760 [43] e RFC-1700.

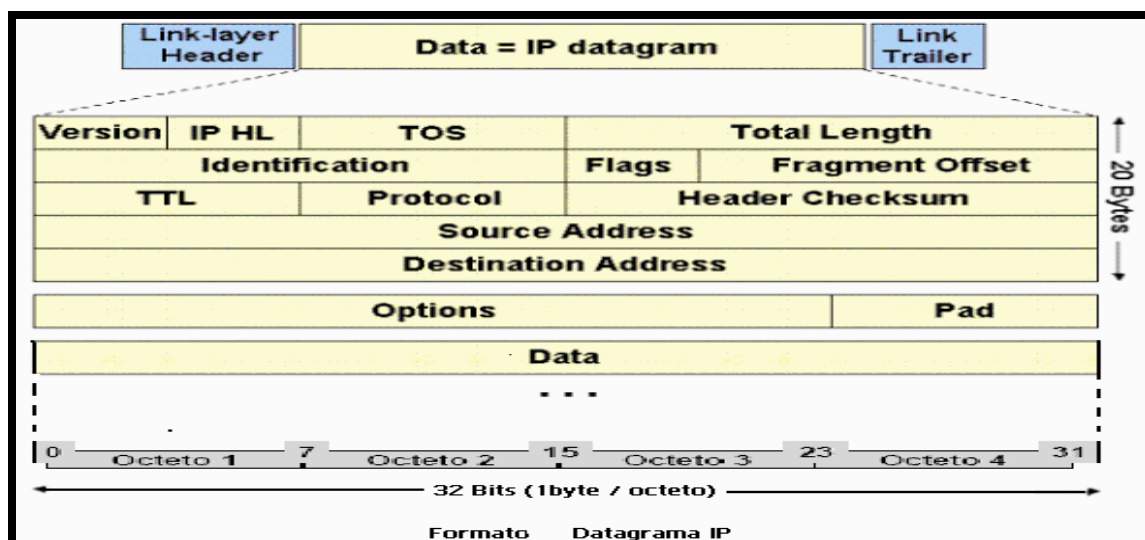


Figura 62 - Formato do cabeçalho IP (Figura readaptada) [7]

O Cabeçalho Checksum (*Header Checksum*): Possui 16 bits, fornece uma verificação da soma do cabeçalho, auxiliando o roteador na detecção de erros de bits em um datagrama. Os dados podem conter erros. Se o cabeçalho *checksum* falha, o datagrama é descartado uma vez que é ele a entidade que descobre o erro. O IP não fornece facilidade de uma comunicação confiável. Não existe nenhum reconhecimento fim-a-fim ou salto a salto. Não existe nenhum controle de erro para dados, só um cabeçalho checksum. Não existe nenhuma retransmissão. Não existe nenhum controle de fluxo.

O Tempo de vida (*TTL – Time to Live*) 8 bits: É uma indicação do tempo de vida que um datagrama deve permanecer em um sistema de Internet; o valor zero indica que o datagrama deve ser destruído. Isto garante que um datagrama não fique circulando indeterminadamente na rede. É fixado pelo remetente do datagrama e reduzido seu valor ao longo da rota onde ele está sendo processado. Se o tempo de vida alcançar o valor zero antes do datagrama alcançar seu destino, e é destruído.

TOS (*Service Type*): Os 8 (oito) bits de tipo de serviço (*Type of Service*) foram incluídos no cabeçalho do IPv4 para poder diferenciar os diferentes tipos de datagramas IP que devem ser distinguidos, presumivelmente, para que possam ser manipulados de maneiras diferentes quando houver sobrecarga. Por exemplo, quando a rede está sobrecarregada, é útil distinguir os datagramas de controle de rede como o ICMP (*Internet Control Message Protocol*) dos datagramas que transportam dados como mensagens HTTP (*Hyper Text Transfer Protocol*). Também é muito útil diferenciar os datagramas em tempo real dos tráfegos do tempo não real. Contudo, recentemente, os roteadores do CISCO

especificam que o serviço a ser fornecido é uma questão de política determinada pelo administrador de roteador. O administrador teria que lidar com as facilidades opcionais providas pelo campo TOS.

Opções (Options): A descrição precedente criou uma simplificação inacessível. Assumiu-se que não havia opções de Internet associadas com o datagrama sendo remontado. A dificuldade com opções é que até o recebimento do primeiro fragmento do datagrama não diz o tamanho do cabeçalho de internet. Isso ocorre porque, enquanto certas opções são copiadas identicamente em cada fragmento de um datagrama, outras opções tais como "*recorde route*", são colocadas apenas no primeiro fragmento. (O primeiro fragmento contem o octeto "0" do datagrama original).

Este campo fornece funções para controle útil em algumas situações, mas desnecessárias para as comunicações mais comuns. As opções incluem providências para *time-stamps*, relatórios de erro e, em especial, roteamento. Este campo é raramente usado porque permite que o cabeçalho IP seja ampliado, não podendo determinar à priori onde começa o campo dos dados.

Até saber o tamanho do cabeçalho de internet, fica-se sem se sabe onde copiar os dados de cada fragmento no *buffer*³³ de remontagem.

Se o primeiro fragmento a chegar for o primeiro fragmento do datagrama, isso não constituirá problema. Caso contrário, existem duas soluções:

- ✓ Primeira: pode-se deixar espaço no *buffer* de remontagem para o tamanho máximo de um cabeçalho de internet. De fato, o tamanho máximo não é tão grande, 64 octetos;
- ✓ Segunda: pode-se apostar que o primeiro fragmento não contém opções. Quando o primeiro fragmento chegar com opções, os dados podem deslocar-se no *buffer* a uma distância suficiente para permitir inserir os remontar os datagramas.

11.4.2 - Fragmentação e remontagem de pacotes a nível IP.

A RFC-791 define que a função ou propósito do Protocolo de Internet (IP) é mover datagramas através de um conjunto de redes interconectadas. Isso é feito pela passagem de

³³ **Buffer:** Espaço de Memória em dispositivos destinado a armazenar pacotes de dados, que esperam processamento.

datagramas de uma camada de Internet a outra, até que alcance o destino. A camada de Internet consiste em *hosts* e *gateways* num sistema de Internet. Os datagramas são roteados individualmente, de uma camada de Internet a outra através de redes baseadas na interpretação dos endereços de Internet.

No roteamento de mensagens de uma camada de Internet até outra, os datagramas podem precisar de atravessar uma rede cujo tamanho máximo de pacotes permitido é menor que o do datagrama. Para contornar esta dificuldade, o mecanismo de fragmentação pelo IP é provido. Ainda segundo a RFC-791, a fragmentação de um datagrama é necessária quando este origina em uma rede local que permite um tamanho de pacote grande e deve atravessar uma rede local que limita pacotes a um tamanho menor para alcançar seu destino.

Um datagrama pode ser marcado como “não fragmentar” (*don't fragment*). Qualquer datagrama uma vez marcado não é fragmentado sob circunstância alguma. Se esse datagrama não pode ser entregue no destino sem ser fragmentado, deve, então, ser descartado, devendo ser informado ao emissor através de ICMP.

O procedimento de fragmentação e remontagem precisa ser capaz de quebrar um datagrama em um número quase arbitrário de pedaços que podem vir a ser remontados mais tarde. O receptor dos fragmentos usa o campo de identificação para assegurar que aqueles fragmentos de diferentes datagramas não sejam misturados [8], [71].

A Figura 63 a seguir ilustra um cenário de fragmentação e remontagem de pacotes a nível do IP.

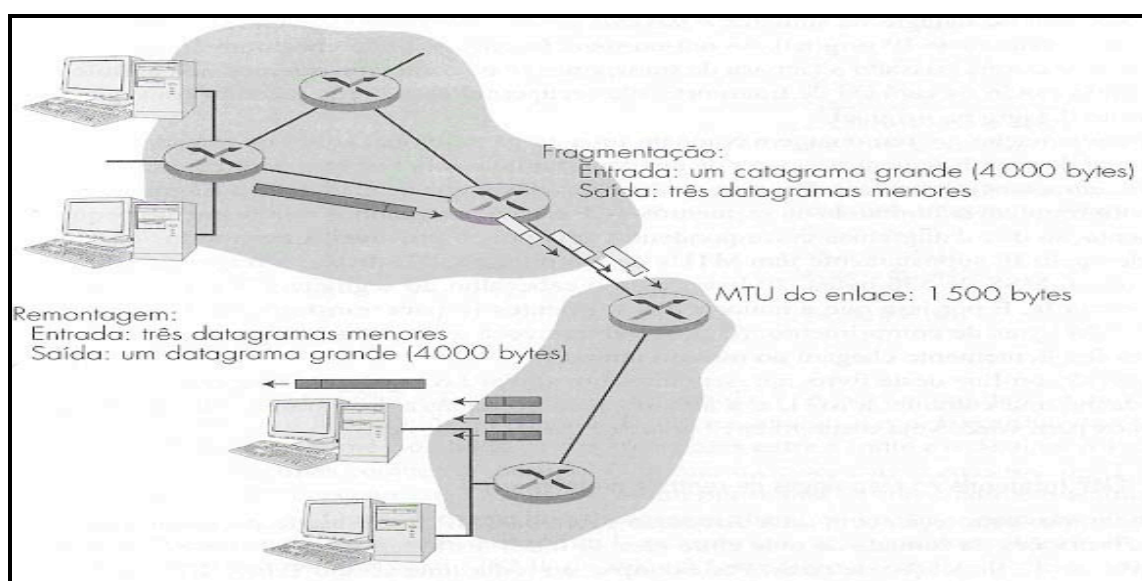


Figura 63 - Fragmentação e remontagem em uma rede de mesmo tamanho de MTU [8]

Na Figura 63, toda a rede possui a mesma capacidade de MTU, neste caso os pacotes sofrerão uma única fragmentação no L3 que seja compatível com a MTU de 1500 bytes, pois a rede toda tem a MTU dessa mesma capacidade. Mais a frente será mostrado o procedimento de fragmentação e remontagem onde a rede possui equipamentos diferentes e de tamanho de MTU diferente.

O fato de que nem todos os protocolos de comunicação entre redes poderem carregar os mesmos tamanhos de pacotes, ou seja, alguns deles têm capacidade de carregar pacotes grandes enquanto que outros não os conseguem, justifica o procedimento de fragmentação dos pacotes. Fragmentos são ditos pacotes / datagramas que são divididos em datagramas menores a fim de serem finalmente carregados por um protocolo específico de nível-2 (enlace), respeitando o seu respectivo MTU, uma vez que o seu tamanho original é maior que o tamanho permitido a ser carregar por um determinado protocolo de enlace de uma rede específica. A MTU (*Maximum Transmit Unit*) corresponde à quantidade máxima de dados que um pacote de camada de enlace pode carregar ao ser transmitido por intermédio de um link de transmissão de uma determinada tecnologia de alta velocidade como Fast/Gigabit Ethernet, levando em consideração a MTU da rede e o “buffer de recepção do host final”, ou seja, a MTU refere-se ao maior tamanho de datagrama que uma camada de um protocolo de comunicação pode transmitir em um link de transmissão de uma interface de rede específica [72]. Um caso a ser ilustrado é o dos protocolos Ethernet. Estes podem carregar até 1500Bytes de dados, enquanto que os pacotes para muitos enlaces de longa distancia não podem carregar mais do que 576 bytes. No caso do protocolo IP que não é confiável e não orientado a conexão, portanto sujeito à falhas, foi desenvolvido o paradigma de encaminhamento de dados que consiste na fragmentação dos pacotes encaminhados separadamente na grande maioria dos casos, uma vez que um datagrama IP é encapsulado dentro do pacote de camada de enlace para ser transportado de um roteador até o roteador seguinte por intermédio de qualquer rota disponível, escolhida apenas com base nas informações locais de cada roteador.

Assim sendo, a MTU do protocolo da camada de enlace coloca um limite bastante restrito no cumprimento do datagrama IP. Esta operação, no entanto, não constitui problema algum. O problema reside no fato de cada um dos enlaces poder, ao longo da rota entre remetente e destinatário, usar diferentes protocolos de enlace e cada um desses protocolos pode ter diferentes MTU. Daí surgem alguns motivos que comprovam a incessante

necessidade da realização de fragmentação. A figura que se segue exemplifica, de forma esquematizada, esse relacionamento de MTU de protocolos de enlace diferente e redes de tecnologia diferentes. Na Figura 64 a seguir cujo cenário representa uma rede de MTU diferentes, admitamos, por exemplo, que a estação geradora de tráfego “A” queira transmitir datagrama de 4000 octetos de dados para estação “B”. Percebe-se que para o datagrama chegar ao destino precisa, necessariamente, de passar por uma rede (Rede-2) de MTU = 1500. Por outro lado o caminho partindo da Rede-1 contém uma MTU = 4500 e a Rede 3 possui uma MTU = 800. Isto demonstra uma variação na ordem de fragmentação devido a existência de redes diferentes, contendo MTU diferentes. Deste modo, podemos dizer que na Rede-2 serão gerados, necessariamente, seis (6) fragmentos, sendo 120 bytes são *overhead*, já que o destino não consegue receber no seu *buffer* dados ora suportados pela MTU da Rede-2 e esta, por sua vez, não possui capacidade de receber dados suportados pela Rede-1.



Figura 64 - Fragmentação e remontagem em uma rede de MTU diferentes

Se a Rede-3 tivesse capacidade de receber o mesmo volume de dados que a Rede-2, seriam gerados, simplesmente, três (3) fragmentos, o que significa que seria gerada menor quantidade de *overhead* na rede devido aos acréscimos de cabeçalhos em cada fragmento. Um datagrama IP pode ter um tamanho de até 65535 bytes. Por outro lado, o IP é um protocolo da camada de rede que deve ser transportado por protocolos de enlace como é o caso do IP sobre ethernet, cujo quadro tem um tamanho máximo (MTU - *Maximum Transmission Unit*) de 1500 bytes, conforme exemplifica a Tabela 41 a seguir. Esta Tabela representa uma rede com tecnologia de enlace provido pelo mesmo protocolo, o protocolo Ethernet, tornando, mas fácil a operação de fragmentação.

Original IP Datagram					
Sequence	Identifier	Total Length	DF May / Don't	MF Last / More	Fragment Offset
0	345	5140	0	0	0

IP Fragments (Ethernet)					
Sequence	Identifier	Total Length	DF May / Don't	MF Last / More	Fragment Offset
0-0	345	1500	0	1	0
0-1	345	1500	0	1	185
0-2	345	1500	0	1	370
0-3	345	700	0	0	555

Tabela 41 - Fragmentação quadro Ethernet [7].

Da Tabela 41, pode-se inferir que: Se somarmos todos os tamanhos dos fragmentos IP, o valor excederá em 60 bytes o tamanho do datagrama IP original. A razão principal do aumento desse comprimento para 60 bytes prende-se com a criação de três cabeçalhos de IP adicionais, uma para cada fragmento depois do primeiro fragmento.

O primeiro fragmento tem um *offset* de 0 (zero) cujo tamanho é de 1500, incluindo 20 bytes para modificação superficial do cabeçalho de IP original.

O segundo fragmento tem um campo *offset* de 185 ($185 \times 8 = 1480$ ou $1480 / 8 = 185$) o que significa que a parcela de dados deste fragmento começa em 1480 bytes no datagrama IP original. O tamanho deste fragmento é de 1500 bytes, incluindo o cabeçalho de IP adicional criado para esse fragmento.

O terceiro fragmento tem um campo *offset* de 370 ($370 \times 8 = 2960$ ou $(1480+148)/8 = 370$) significando isto que a parcela de dados deste fragmento começa em 2960 bytes no datagrama IP original. O tamanho desse fragmento é de 1500 bytes, incluindo o cabeçalho de IP adicional criado para esse fragmento.

O quarto fragmento tem um campo *offset* de 555 ($555 \times 8 = 4440$) o que significa que a parcela de dados deste fragmento começa em 4440 bytes no datagrama IP original. O tamanho deste fragmento é de 700 bytes, incluindo o cabeçalho de IP adicional criado para esse fragmento. Só quando o último fragmento for recebido é que o tamanho do datagrama IP original poderá ser determinado. O fragmento *offset* deste último fragmento (555) resulta em dados *offset* de 4440 bytes no datagrama IP original.

Então, se adicionarmos os bytes de dados do último fragmento ($680 = 700 - 20$), isso vai perfazer 5120 bytes, que correspondem a parcela de dados do datagrama IP original. Então, somando 20 bytes para um cabeçalho IP, igualar-se-á o tamanho do datagrama IP original ($4440 + 680 + 20 = 5140$) [7],[73]. Como nem todos os pacotes devem ser fragmentados, por forma a permitir que muitos datagramas marcados como

”*don’t fragment*”, sejam realmente enviados sem ser fragmentados, evitando, assim, o risco de serem descartados pelo roteador, a RFC-1191 [73] apresenta uma tentativa de resolução. Uma vez ocorrida a fragmentação de pacotes, há de haver, necessariamente, uma reorganização e reintegração dos fragmentos, voltando ao datagrama ou pacote original. Por isso, esse processo é denominado de remontagem dos pacotes e os algoritmos aplicados nesta tarefa são discutidos na subseção seguinte.

11.4.3 - Remontagem de pacotes fragmentados

Para remontar os fragmentos de um datagrama em uma camada IP (por exemplo, em um host de destino) os projetistas IPv4 criaram os campos de **Identificação**, **Fonte**, **Destino**, e **Protocolo** (além dos campos *flags* e *fragment offset*), combinando, deste modo, datagramas Internet que têm todos o mesmo valor para os quatro campos atrás mencionados.

A combinação é feita colocando uma parcela de dados de cada fragmento na posição indicada relativa ao “*fragment offset*” naquele fragmento do cabeçalho de Internet. O primeiro fragmento terá o “*fragment offset*” zero e o último fragmento terá o “*more-fragment flag*” resetado a zero [71]. Os fragmentos precisam de ser remontados antes de chegarem à camada de transporte no destino. Os protocolos de transporte (TCP e UDP) esperam receber da camada de rede *segmentos*³⁴ completos e não segmentos fragmentados. Os projetistas de IPv4 perceberam que a remontagem e a possível fragmentação dos datagramas nos roteadores introduziriam uma complicação significativa no protocolo e colocariam um freio no desempenho do roteador. Seguindo o princípio da conservação da simplicidade da camada de rede, os projetistas do IP versão quatro (IPv4) decidiram passar a tarefa de remontagem de datagramas aos sistemas finais, preparando os roteadores da rede. Quando um hospedeiro destinatário recebe uma série de datagramas da mesma fonte, ele precisa determinar se, de entre esses datagramas, alguns são fragmentos de um datagrama original de maior tamanho. Se ele, de fato, determinar que alguns desses datagramas são fragmentos, deve determinar, adicionalmente, quando recebeu o último datagrama e como os fragmentos recebidos devem ser remontados para voltar à forma do datagrama original [8],[71].

Quando um datagrama é criado, ele é marcado pelo hospedeiro remetente com um número de identificação bem como um endereço da fonte e do destino. O hospedeiro remetente incrementa o número de identificação para cada datagrama que envia. Quando

34

Segmento: Unidade de informação utilizada pela Camada de Transport

um roteador precisa de fragmentar um datagrama, ele marca com um endereço da fonte, o endereço do destino e o número de identificação do datagrama original a cada datagrama (fragmento) resultante da fragmentação. Quando o destinatário recebe uma série de datagramas do mesmo hospedeiro remetente, ele pode examinar o número de identificação dos datagramas para determinar quais deles são, na verdade, fragmentos de um mesmo datagrama de tamanho maior.

Como o IP é um serviço não confiável, é possível que um ou mais desses fragmentos jamais cheguem ao destino. Por essa razão, para que o hospedeiro de destino fique absolutamente seguro de que recebeu o último fragmento do datagrama original, esse último datagrama tem um bit de *flag* ajustado para zero (0) ao passo que todos os outros fragmentos tem um bit de *flag* ajustado para (1) um. Além disso, para que o hospedeiro destinatário possa determinar se está faltando algum segmento (e possa remontar os fragmentos na ordem correta) o campo de deslocamento (*fragment offset*) é usado para especificar a localização exata de fragmento no datagrama IP original [23]. O processo de remontagem, segundo a RFC-815, é um mecanismo que obedece a determinado algoritmo de remontagem específica, sendo necessário definir alguns termos. Um datagrama parcialmente remontado consiste em certas sequências de octetos que já chegaram e certas áreas que ainda virão. Nós referir-nos-emos a essas áreas que faltam como "lacunas". Cada lacuna deve ser caracterizada por dois números, *hole.first*, é o número do primeiro octeto da lacuna e, *hole.last*, o número do último octeto da lacuna.

Este par de números é chamado de "descriptor de lacuna" e assumiremos que todos os descriptors de lacunas para um datagrama particular estão em uma lista de descriptors de lacunas. Existem para tanto, algoritmos que demonstram como é a operação desses processos. Abaixo segue a descrição de um algoritmo semi-formal.

11.4.4 – Principio do algoritmo de remontagem de pacotes

A forma geral do algoritmo é a seguinte:

- Quando chega um novo fragmento do datagrama, este, possivelmente, irá preencher uma ou mais das lacunas existentes. Nós examinaremos cada uma das entradas na lista de descriptors de lacuna para ver se a lacuna em questão é eliminada por este fragmento. Se isso acontecer, nós apagaremos a entrada da lista. Eventualmente, um fragmento pode chegar e eliminar todas as entradas da lista. Nesse ponto o datagrama estará completamente remontado e poderá ser passado para a outra camada da pilha de protocolos.

O algoritmo pode ser descrito em duas partes:

- Na primeira parte nós mostraremos a sequência de passos que são dados quando um novo fragmento chega para determinar se nenhuma das lacunas existentes foi preenchida pelo novo fragmento.

✓ Na segunda parte dessa descrição, mostraremos um algoritmo simples para administração da lista de descritores de lacunas.

11.4.4.1 - Parte 1: Algoritmo de processamento de fragmentos

Um fragmento que chega pode preencher, de várias maneiras, qualquer das lacunas existentes, ou pode, simplesmente, completar uma lacuna. Ele pode, alternadamente, deixar algum espaço sobrando no início ou no final de uma lacuna existente; ele pode, ainda, estar no meio de uma lacuna existente, separando a lacuna no meio e deixando uma pequena lacuna em cada extremidade. Devido a essas possibilidades, vários testes devem ser feitos quando um novo fragmento chega conduzindo a um algoritmo bastante complicado. O algoritmo pode comparar cada lacuna com o fragmento que chega a quatro testes apenas. Começa-se com o algoritmo aonde chega o primeiro fragmento do datagrama. Cria-se uma área vazia de *buffer* de dados e coloca-se uma entrada em sua lista de descritores de lacunas; a entrada descreve o datagrama como completamente vazio. Neste caso, *hole.first* é igual a zero e *hole.last* é igual a infinito. Os oito passos seguintes são usados para inserir cada um dos fragmentos que chegam na área de *buffer* onde o datagrama está sendo construído. O fragmento que chega é descrito por *fragment.first*, o primeiro octeto do fragmento, e *fragment.last*, o último octeto do fragmento.

- I. Seleciona o próximo descritor de lacuna na lista de descritores de lacunas. Se lá não existirem mais entradas vá para o passo 8.
- II. Se o *fragment.first* é maior que o *hole.last* vá para o passo 1.
- III. Se o *fragment.last* é menor que o *hole.first* vá para o passo 1. (Se os passos 2 e 3 forem verdadeiros então o fragmento recém-chegado não irá sobrepor a lacuna e, neste caso, precisamos, no futuro, prestar atenção a esta lacuna. Nós retornamos ao início do algoritmo onde selecionamos a próxima lacuna a ser examinada.)
- IV. Apagar a entrada corrente da lista de descritor de lacunas. (Quando os passos 2 e 3 forem falsos, o fragmento recém-chegado não interage com a lacuna de maneira alguma. Portanto, o descritor corrente deixa de ser válido. Nós

destruiremo-lo e nos dois passos seguintes determinaremos se é necessário criar quaisquer novos descritores de lacunas.)

- V. Se *fragment.first* for maior que *hole.first* então cria-se um novo descritor de lacunas "*new_hole*" com "*new_hole.first*" igual a "*hole.first*" e "*new_hole.last*" igual a "*fragment.first*" menos 1. - (Se o teste no passo cinco for verdadeiro então a primeira parte da lacuna original não será preenchida por este fragmento e criamos um novo descritor para esta lacuna).
- VI. Se "*fragment.last*" for menor que "*hole.last*" e "*fragment.more_fragments*" for verdadeiro então cria-se um novo descritor de lacunas "*new_hole*" com "*new_hole.first*" igual a "*fragment.last*" mais um e "*new_hole.last*" igual a "*hole.last*". - (Esse teste é o espelho do passo cinco com uma característica adicional. Inicialmente, nós não sabíamos qual seria o tamanho do datagrama remontado e, portanto, criamos uma lacuna do zero ao infinito). Eventualmente, nós receberemos o último fragmento do datagrama. Nesse momento, o descritor de lacunas que alcança a distância do último octeto do *buffer* ao infinito pode ser descartado. O último fragmento contém o bit zero no *flag more-fragments*. (O teste desse bit, nessa sentença, nos precavé de criar um descritor para uma lacuna desnecessária que descreve um espaço do final do datagrama ao infinito).
- VII. Vá para o passo 1.
- VIII. Se a lista de descritores de lacunas estiver vazia o datagrama estará completo. Passe para a camada superior da pilha de protocolos. Se não retorne [RFC-815] [23].

11.4.4.2 - Parte 2: Administrando a lista de descritores de lacunas.

O mais complicado desses 8 (oito) passos do algoritmo não é a performance dos testes aritméticos, mas sim a adição e remoção de entradas na lista de descritores de lacunas. Pode-se imaginar uma implementação em que os administradores de *buffer* de pacotes são várias vezes mais complicados que o resto do algoritmo, desde que não haja especificação do número de descritores de lacunas que existirá para um datagrama durante a remontagem. Há uma maneira simples de lidar com descritores de lacunas. Ponha cada descritor de lacuna nos primeiros octetos da lacuna em si. Observe que pela definição do algoritmo de remontagem o tamanho mínimo de uma lacuna é de oito octetos. Para armazenar *hole.first* e *hole.last* requerer-se-á dois octetos cada.

Dois octetos adicionais serão necessários para cada linha das entradas da lista de descritores de lacunas. Isso é apenas um dos problemas óbvios na estratégia de

armazenamento. Deve-se executar o algoritmo de oito passos acima antes de se copiar os dados do fragmento no *buffer* de remontagem. Se se copiar o dado primeiro ele pode quebrar um ou mais descritores de lacunas. Uma vez que executado o algoritmo acima, qualquer descritor de lacunas que iria quebrar-se, torna-se obsoleto. Dispensar os descritores de lacunas através do buffer de remontagem requer que os mesmos estejam ordenados na linha em alguma ordem da lista para que possam ser encontrados. Isso implica que haja um ponteiro para o início da lista. Em muitos casos, esse ponteiro pode ser armazenado em algum bloco de descritor cuja implementação associa-se a cada *buffer* de remontagem. Se tal armazenamento for possível, um outro artifício a ser utilizado seria armazenar o cabeçalho da lista em uma parte do cabeçalho de internet no buffer de remontagem que não se usa mais. Uma localização óbvia é o campo de *checksum*. Quando o fragmento final do datagrama chega, o tamanho do campo do pacote no cabeçalho de internet deve ser preenchido.

11.4.4.2.1 - O algoritmo de remontagem de pacotes (RFC-815)

Além do algoritmo descrito acima há duas partes do processo de remontagem a saber:

- Primeira, quando um fragmento chega é necessário encontrar um buffer de montagem associado ao fragmento. Isso requer algum mecanismo para buscar em todos os buffers de remontagem existentes. O *buffer* de remontagem correto é identificado pela igualdade dos seguintes campos: o endereço de internet local, o ID do protocolo e o campo de identificação. A parte final do algoritmo corresponde a algum tipo de mecanismo baseado em tempo que decrementa o campo do tempo de vida de cada datagrama parcialmente remontado, para que datagramas incompletos que tenham fragmentos em falta possam ser descartados. Pode-se criar outra versão que fique viva uma vez por segundo e decrementa o campo de cada datagrama por um ou possa ler o “*clock*” quando cada primeiro fragmento chega e enfileira algum tipo de chamada de tempo, utilizando qualquer mecanismo apropriado para descartar o datagrama.

Toda a técnica de fragmentação de pacote, requer uma outra técnica para que os mesmos fragmentos possam vir a ser reagrupados na ordem certa. Acham-se descritos acima os algoritmos usados para esse fim. Conforme mencionei anteriormente, uma vez conceituada a fragmentação em nível IP, o capítulo seguinte abordará a questão de fragmentação com intercalação em enlace Frame Relay. Desta forma, o capítulo seguinte irá focar estes dois assuntos.

12 - CAPÍTULO XII - CONTEXTUALIZAÇÃO TEÓRICA - CODECS, RTP e cRTP.

*“As coisas não são boas ou ruins;
o pensamento é que as fazem assim”*
– William Shakespeare

12.1 - CODECS

Ao longo do tempo, diversos codificadores (Codecs) de voz foram projetados para poderem ajudar a aumentar a eficiência do compartilhamento de diversas comunicações telefônicas em um link compartilhado. Estes codificadores são popularmente conhecidos como codecs. Os codecs podem ser classificados em duas categorias distintas:

- ✓ Codecs de forma de onda e,
- ✓ Codecs paramétricos.

No seio dessas duas grandes categorias, existem, entretanto, os codecs de voz (que foram implementados para suportar certo nível de perda enquanto que outros não) com perda e os sem perda. Em resumo, os Codecs de forma de onda fornecem um sinal codificado o mais próximo possível do sinal analógico original. Já os paramétricos modelam o sistema que gera o sinal de voz original e enviam apenas parâmetros deste modelo, sendo a maioria desses parâmetros baseados em predição linear (*Linear Prediction Code - PC*) permitindo, assim, boas taxas de compressão [6].

O método, entretanto, mais usado para a avaliação da qualidade da voz através de codecs é conhecido como MOS (*Mean Opinion Score*). Segundo as Recomendações ITU-T [34], [90] o método se baseia na análise subjetiva de um conjunto de avaliadores que atribuem uma pontuação entre 1 (um) considerado ruim e 5 (cinco) considerados excelentes para uma qualidade da fala que é escutada através de um meio eletrônico analógico ou digital. A qualidade é medida através da média ponderada dos valores de pontuação [35].

12.1.1 – FILOSOFIA DOS CODEC's USADOS NOS TESTES

Abaixo segue uma breve descrição teórica de alguns CODECS usados durante os testes. A principal função dos CODECs é comprimir os dados de um arquivo de áudio ou vídeo para armazenamento ou transmissão. CODECs são frequentemente utilizados em vídeos-conferência e aplicações de fluxo de mídia. O conversor Analógico-Digital de uma câmera de vídeo converte os sinais analógicos em sinais digitais, que são passados por um compressor de vídeo para transmissão digital ou armazenamento.

O equipamento que recebe essa mídia passa os dados por um “descompressor” de vídeo e depois pelo conversor Digital-Analógico para, por exemplo, mostrá-los em uma televisão. Em seguida a descrição de alguns codecs utilizados nos testes de VoIP. Nessas descrições, percebe-se da relevância que é dada aos seus aspectos principais com relação à provisão de serviços de voz sobre IP, entretanto, não descrito, neste trabalho todas as particularidades dos codecs.

12.1.1.1 - O CODEC G711- μ -law (64kbps)

O codificador PCM (*Pulse Code Modulation*) foi padronizado pelo ITUT (*Internacional Telecommunication Union - Telecommunication standardization sector*) na sua recomendação G.711 ITU-T [95]. É um codec de forma de onda simples e de excelente qualidade de reprodução da voz. A voz é amostrada na frequência de 8kHz [88] e possui um delay típico do algoritmo de codificação na ordem de 0,125ms. Cada amostra é quantizada com 8bits, a uma taxa de bits ³⁵ de 64kbps. A sua complexidade não atinge 1MIPS.

Os quadros são compostos de 160 amostras (160 Bytes) o que implica em atraso de 20ms para formação do pacote [35]. Dispõe de compactação mínima com perda, sem modelagem e também sem buffer de armazenamento. Este é o unico que permite que o sinal seja codificado mais próximo do sinal analógico original. Este codec, à

35

Taxa de BITS: Medida dada a qualidade do tamanho final de um arquivo comprimido como um codec com perda e representada normalmente em unidade de kbps. Em um codec, 1kbps significa que a cada segundo, o codec tem 1000bits do arquivo final para utilizar, então se um arquivo de som tiver 8 segundos ele ‘e comprimido a uma taxa de 1kbps, fazendo com que o arquivo final tenha um tamanho de 8kbps que equivale a um 1byte. A relação taxa de bit ‘e diretamente proporcional a qualidade do arquivo final.

semelhança do codec G722 (64kbps) [96], ocupa mais banda em uma FRF.12 do que quaisquer outros codecs, ou seja, este codec não é aconselhado para enlaces de baixa capacidade.

12.1.1.2 -O CODEC G726 (32kbps)

A Recomendação G.726 ITU-T [91] usa descodificadores de forma de onda em conjunto com a predição da codificação ADPCM (*Adaptive Differential Pulse Code Modulation*). De forma análoga ao PCM, o sinal é amostrado a uma taxa de 8kHz, com uma maior compactação do sinal de voz, permitindo alcançar taxas de 16, 24, 32 e 40kbps [88]. O seu atraso máximo de codificação chega aos 0,25ms.

A complexidade dos algoritmos de compressão é mediana, na ordem de 10,54 MIPS³⁶ com perda. Esse Codec ocupa o menor consumo de banda do que o G711 apesar de ambos possuírem qualidades semelhantes [97], conforme evidencia a Tabela 42 a seguir.

Codec Information				Bandwidth Calculations					
Codec & Bit Rate (Kbps)	Codec Sample Size (Bytes)	Codec Sample Interval (ms)	Mean Opinion Score (MOS)	Voice Payload Size (Bytes)	Voice Payload Size (ms)	Packets Per Second (PPS)	Bandwidth MP or FRF.12 (Kbps)	Bandwidth w/cRTP MP or FRF.12 (Kbps)	Bandwidth Ethernet (Kbps)
G.711 (64 Kbps)	80 Bytes	10 ms	4.1	160 Bytes	20 ms	50	82.8 Kbps	67.6 Kbps	87.2 Kbps
G.729 (8 Kbps)	10 Bytes	10 ms	3.92	20 Bytes	20 ms	50	26.8 Kbps	11.6 Kbps	31.2 Kbps
G.723.1 (6.3 Kbps)	24 Bytes	30 ms	3.9	24 Bytes	30 ms	33.3	18.9 Kbps	8.8 Kbps	21.9 Kbps
G.723.1 (5.3 Kbps)	20 Bytes	30 ms	3.8	20 Bytes	30 ms	33.3	17.9 Kbps	7.7 Kbps	20.8 Kbps
G.726 (32 Kbps)	20 Bytes	5 ms	3.85	80 Bytes	20 ms	50	50.8 Kbps	35.6 Kbps	55.2 Kbps
G.726 (24 Kbps)	15 Bytes	5 ms		60 Bytes	20 ms	50	42.8 Kbps	27.6 Kbps	47.2 Kbps
G.728 (16 Kbps)	10 Bytes	5 ms	3.61	60 Bytes	30 ms	33.3	28.5 Kbps	18.4 Kbps	31.5 Kbps
G722_64k(64 Kbps)	80 Bytes	10 ms	4.13	160 Bytes	20 ms	50	82.8 Kbps	67.6Kbps	87.2 Kbps
ilbc_mode_20 (15.2Kbps)	38 Bytes	20 ms	NA	38 Bytes	20 ms	50	34.0Kbps	18.8 Kbps	38.4Kbps
ilbc_mode_30 (13.33Kbps)	50 Bytes	30 ms	NA	50 Bytes	30 ms	33.3	25.867 Kbps	15.73Kbps	28.8 Kbps

Tabela 42 - Cálculos de Banda em enlace FRF12 de acordo com os Codecs [5],[3]

(MIPS) Um algoritmo de compressão de voz é normalmente avaliado em quatro quesitos:

- A eficiência, a complexidade, o atraso e a qualidade. O MIPS é a grandeza de medida da complexidade do algoritmo que refere a medida disposta em Milhões de Instruções por Segundo (MIPS) necessárias na codificação do sinal.

Esse codec, não obstante ser ainda muito usado em sistemas telefônicos e transmissão de voz que exige pouco processamento, tem perdido espaço para o codec G.729, devido a sua incapacidade de trabalhar com bandas passantes baixas, comparativamente ao G.729.

Para a taxa de 32 kbps e quadros de 80 bytes o tempo necessário para se formar um quadro é de 20ms [35] e, se aplicado a compressão de cabeçalho, ocupará 35.6 Kbps de banda passante em enlace Frame Relay Fórum v12 conforme a Tabela 42 acima.

12.1.1.3 - O CODEC G723.1 (6.3kbps)

A ITU-T [32] define dois codificadores paramétricos baseados em técnicas de predição *Algebraic Code Excited Linear Prediction-(ACELP)* com uma taxa de 5,3 kbps e predição *Multi Pulse-Maximum Likelihood Quantization-(MP-MLQ)* para a taxa de 6,3 kbps e a frequência de amostragem é de 8 kHz.

Este codec possui entre 10 e 11 MIPS como média da complexidade dos algoritmos de compressão. Se o codec for usado a uma taxa de 6,3kbps, serão então usados quadros de 24 Bytes, podendo, assim assegurar uma boa audibilidade a um tempo de aproximadamente os sensíveis 30ms de *jitter*, conforme a Tabela 43 a seguir.

Codec	Voice Payload Size (ms)	Voice Payload Size (Bytes)	Comments
G.711	20 ms (default)	160 Bytes	Notice that the codec bit rate is always maintained. For example: G.711 codec = $[240 \text{ bytes} * 8(\text{bits/bytes})] / 30 \text{ ms} = 64 \text{ Kbps}$
	30 ms	240 Bytes	
G.729	20 ms (default)	20 Bytes	
	30 ms	30 Bytes	
G.723	30 ms (default)		

Tabela 43 - Atraso de formação de quadro em G723[5]

O G723.1 é a extensão da Recomendação G.721 de modulação adaptativa diferencial de código de pulso a 24kbps e 40kbps para a aplicação em equipamento multiplexação digital de circuito. Opera, igualmente, a frequência de amostragem de 8kbps. Já no estado obsoleto, foi substituído pelo G.726 [88],[33]. O tempo necessário para se formar um quadro usando este codec é por *default* 30ms, o que o deixa em desvantagem em relação aos demais [35].

12.1.1.4 - CODEC G729-b (8kbps)

A recomendação ITU-T G729b, permite a codificação de voz em 8kbps usando a técnica de predição - *Conjugate-Structure Algebraic Code Excited Linear Prediction* (CS-ACELP). O sinal é amostrado a uma taxa de 8khz e cada amostra é quantizada com 8bits a uma taxa de 8kbps, com o tempo necessário para formar um quadro em 10ms e aplicado a compressão de cabeçalho em enlace FRF.12 que tem a menor ocupação de banda na ordem de 11.6 Kbps e com baixo delay na ordem de 15ms a 20ms para formação de quadro [88],[35]. Possui também um atraso máximo de codificação típico do algoritmo de 0.250ms, apresentando assim vantagens quando comparado aos demais acima mencionados. Ainda este codec, dispõe de alto nível de compactação de voz, permite a modelagem do sistema que gera o sinal de voz e envia apenas os parâmetros desse modelo que necessita de armazenamento [69].

Essas usadas pela OP, são licenciadas, podendo trabalhar com o asterisk normalmente, entretanto a versão *free* que igualmente é suportado pelo Asterisk e o anexo “d” – G729d.

O codec G729b é usado nos dias de hoje em larga escala devido as suas necessidades de largura de banda baixa, combinando assim ao uso principalmente em *Voice over Internet Protocol* (VoIP) onde a banda deve ser conservada. O G.729 no seu anexo “b” (G729b), - prevê um método de compressão de silêncio que possibilita habilitar o método de detecção de atividade de voz através do módulo VAD – (*Detect Voice Activity*) e detecta o ruído de ambiente através do módulo DTX (*Discontinuous Transmission*) e os elimina da transmissão, ao mesmo tempo este adiciona ao som do ouvinte um ruído de conforto através do módulo do decodificador CNG (*Confort Noise Generator*). Este é usado para detectar atividade de sinal de voz no canal, podendo ser controlada a taxa de transmissão de acordo com o interesse do operador [92],[93].

12.2 - Protocolo RTP (*Real Time Protocol*) e a sua compressão

O RTP é um protocolo de nível de transporte utilizado para transportar aplicações multimídias contínuas de tempo real em uma conexão ponto a ponto. Além da utilização em comunicação ponto a ponto, pode também ser usada em uma comunicação *multicast* utilizando o IP com uma faixa reservada para grupos *multicast*.

Este protocolo, contudo, não reserva recursos para as aplicações e também não garante (QoS). Por conta dessas características ele é utilizado junto com o protocolo – *Real Time Control Protocol* – (RTCP), permitindo que a comunicação seja monitorada. Os protocolos RTP e RTCP, apesar de serem usados em paralelo, os pacotes de cada um deles são transmitidos de forma independente.

O RTP diferencia as mídias enviando-as em diferentes sessões RTP ainda que sejam da mesma comunicação. Um caso típico são as sessões de videoconferência. Os pacotes de áudio serão transmitidos por uma sessão RTP e os pacotes imagens em outra sessão RTP diferente e independente. O RTP usa um importante componente chamado de *Translator*. Este tradutor é utilizado quando um usuário se encontra bloqueado para pacotes como, por exemplo, atrás de um *Firewall* ou em comunicações entre participantes utilizando IP e UDP.

Neste caso o tradutor é posicionado de cada lado da barreira; o primeiro receberá o pacote e fará a sua tradução para um formato que tenha permissão de passar; o segundo tomará esta forma traduzida, transformando-a de maneira necessária para entendimento dos receptores e transmiti-la-á para destino unicast ou multicast. A outra grande diferença deste protocolo é a sua sessão de *timestamp* do seu cabeçalho, que será descrito na Tabela 44 a seguir [84].

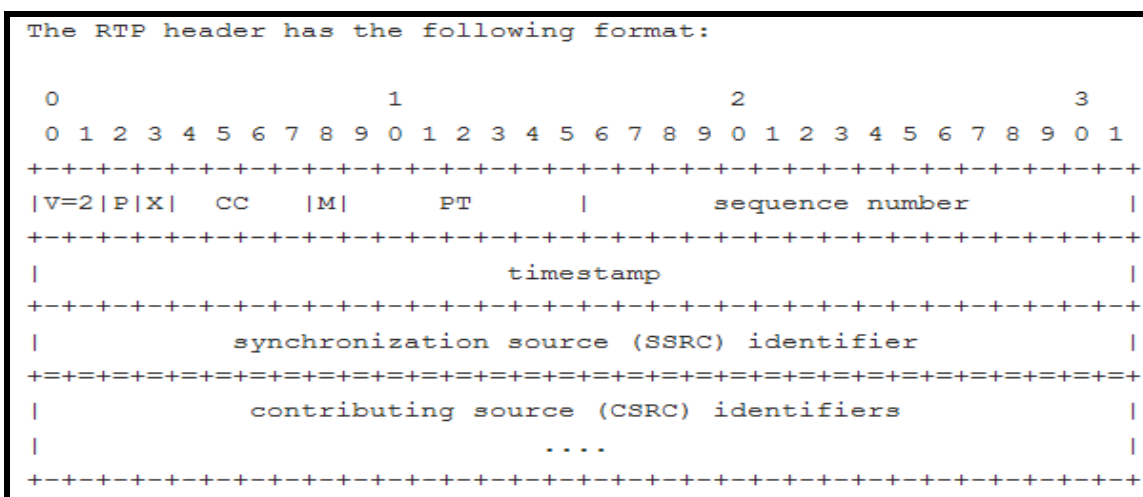


Tabela 44 - Formato de cabeçalho RTP [84]

12.2.1 - Descrição dos campos do cabeçalho RTP [84],[89]

De acordo com a tabela acima, segue a descrição resumida dos seus respectivos campos.

Versão - *Version* (V): 2bits;

Assim como nos demais cabeçalhos de protocolos, este campo identifica a versão de RTP. Este cabeçalho refere-se à versão 2 deste protocolo. A versão 1 foi usada pelo primeiro *draft* do RTP. A versão 0 foi inicialmente desenvolvida para o VAT (ferramenta de transmissão de áudio);

Enchimento - *Padding* (P): 1bit

Este pode ser necessário a alguns algoritmos de criptografia com tamanhos de bloco fixo ou ainda para o transporte de diversos pacotes RTP em uma camada inferior à das unidades do protocolo. Este bit é setado quando existem um ou mais octetos adicionais ao final do pacote que não fazem parte dos dados. Os últimos octetos deverão ser ignorados, pois estão ali por causa de alguns algoritmos de encriptação que precisam de um tamanho fixo dos blocos ou para carregar vários frames RTP. O último octeto de que sofreu o *padding* terá necessariamente as informações de quantos octetos foram inseridos.

Extensão- *Extension* (X): 1bit;

Se for setado a 1 (um) o cabeçalho fixado será seguido de apenas uma extensão de cabeçalho;

Contador - *CSRC Count* (CC): 4bits;

Identifica a quantidade de identificadores CSRC (*Contributing source Count*) presentes no cabeçalho; estes seguem fixo no cabeçalho;

Marcador - *Marker* (M): 1bit;

Este bit pode ser usado pela aplicação para marcar determinados pacotes.

A interpretação do marcador é definida por um perfil que é planejado para permitir que eventos significativos como limites dos quadros sejam marcados no fluxo de pacote.;

Tipo de dados - *Payload Type* (PT): 7bits

Este campo identifica o formato do *payload* RTP e determina o tipo de dados que há no pacote e como deve ser interpretado pela aplicação;

Número Sequencial (*sequence number*) - 16 bits

Este é incrementado de um a cada pacote RTP enviado e pode ser usado pelo receptor para detectar perda e recuperação de sequência de pacote. Ordena os pacotes de uma

comunicação, sendo que o primeiro pacote recebe um número sequencial aleatório e os seguintes recebem o número sequencial do pacote imediatamente anterior incrementado de 1 (uma) unidade;

Carimbo de Tempo (timestamp) - 32 bits

Reflete o instante de amostragem em que o primeiro octeto dos pacotes dados RTP foram gerados. São utilizados para eventos de registro em sistemas de arquivos; data e hora podem significar a data armazenada / hora de criação ou modificação de um arquivo;

SSRC: Identificador (*Synchronization Source*) - 32 bits

Este campo identifica as fontes de sincronização. Deve ser escolhido aleatoriamente, com a intenção de que não haja duas fontes de sincronização na mesma sessão RTP que terá o mesmo identificador SSRC. Assim, cada participante de uma sessão RTP escolhe aleatoriamente um identificador SSRC que irá identificá-lo dentro desta sessão frente aos outros participantes;

CSRC: Fonte Contribuinte (*Contributing Source*) - Lista: 0 a 15 itens, 32 bits cada.

A lista CSRC identifica as fontes que contribuem para a formação da carga de dados contidos neste pacote. O número de identificadores é dado pelo campo CC. Se houver mais de 15 fontes de contribuição, apenas 15 podem ser identificados. Identificadores CSRC são inseridos pelos (*mixers*) misturadores, usando os identificadores de fontes contribuintes SSRC;

12.2.2 - RTP Compressão de cabeçalho

O tamanho do cabeçalho RTP é de 12 bytes, o do UDP de 8bytes e do IP de 20 bytes, totalizando 40 bytes. A Tabela 45 a seguir mostra a disposição dos protocolos e dos respectivos cabeçalhos. Quanto aos *payloads* variam de acordo com o codec utilizado.

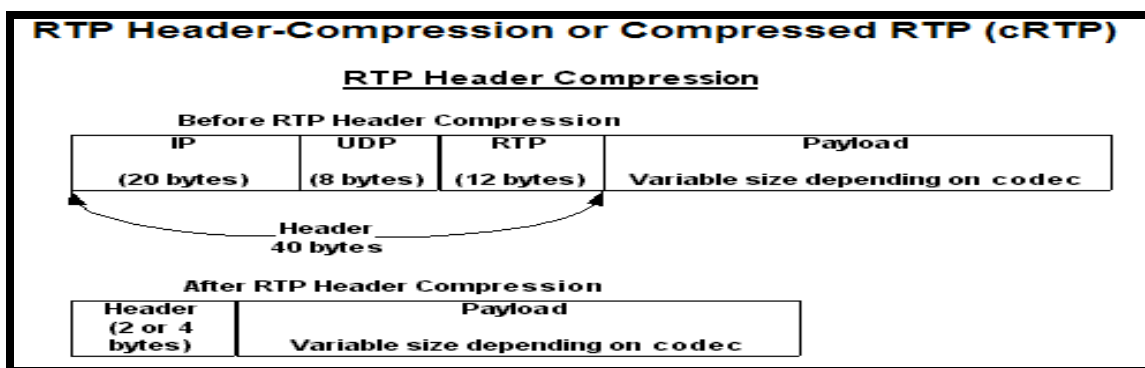


Tabela 45 - RTP Compressão de cabeçalho [5]

Considerando o *payload* IP de 20 bytes, teríamos só de cabeçalho 66,66% da banda da conexão. Como parte de solução usa-se o protocolo CRTP, que na maior parte do tempo, consegue uma compressão de cabeçalho de 40 para 2 bytes ou para 4 se considerarmos o *checksum* UDP. Essa compressão corresponde a uma redução de até 95% na sobrecarga (*overhead*) referente aos cabeçalhos. A operação cRTP acha-se ilustrada na Figura 65 a seguir. O tráfego total destinado a uma determinada interface é classificado, sendo separado para compressão, o que for RTP. O tráfego RTP é, então, processado num compressor e colocado novamente na fila para ser transmitido [83] [98].

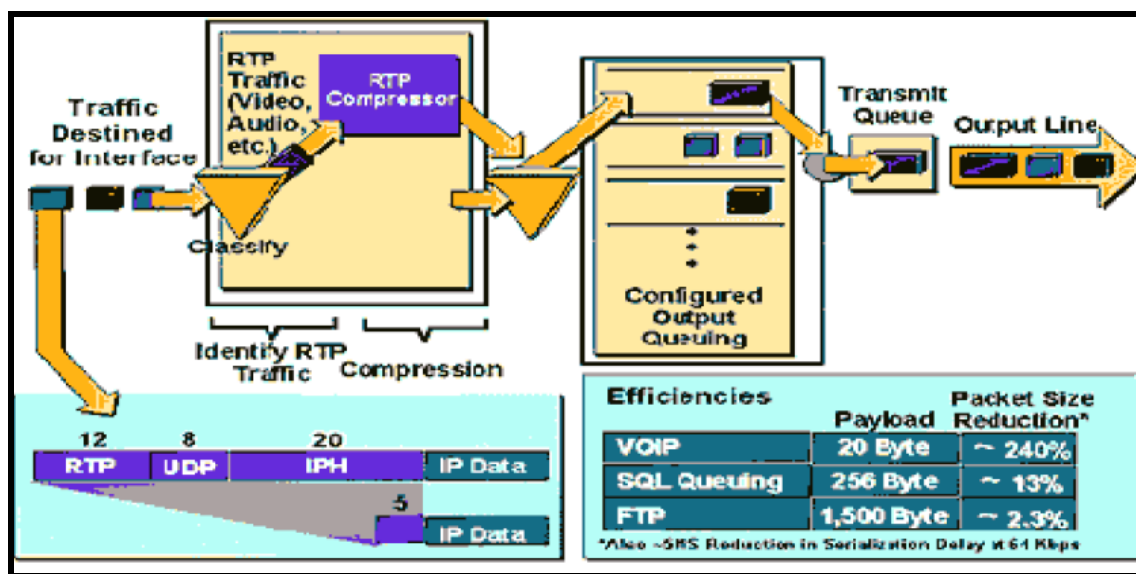


Figura 65 - Separação de tráfego RTP para compressão de cabeçalho [98].

A compressão VoIP é normalmente habilitada nas interfaces seriais nos equipamentos Cisco, principalmente, quando se lida com equipamentos cujas conexões de acesso são de baixa velocidade na ordem de alguns Kbps a 2Mbps [84],[89]. Para efeito de compressão de cabeçalho, segue a subseção 12.2.2.1 que descreve os cabeçalhos dos protocolos que são comprimidos durante os testes todos.

12.2.2.1 – Cálculo de Tamanho de cabeçalhos e ocupação de banda em FRF.12, Ethernet.

Para os testes de cRTP foram levados em conta a contagem do valor numérico do cabeçalho de alguns protocolos. Abaixo segue a demonstração do cálculo, com base na Tabela 46 acima - Cálculos de Banda em enlace FRF12 de acordo com os Codecs” [3]:

- ✓ 40 bytes de cabeçalho sendo IP (20 bytes) / *User Datagram Protocol* (UDP) (8 bytes) / *Real-Time Transport Protocol* (RTP) (12 bytes) cada, respectivamente.
- ✓ *Compressed Real-Time Protocol* (cRTP) reduz os cabeçalhos de IP/UDP/RTP para 2 ou 4bytes (cRTP não é avaliado sobre Ethernet).
- ✓ 6 bytes de cabeçalho para *Multilink Point-to-Point Protocol* (MP) or FRF.12 L2.
- ✓ 1 byte para finalizar o frame do *flag* em MP e *frames* do *Frame Relay*.
- ✓ 18 bytes de cabeçalho de Ethernet L2, incluindo 4 bytes de *Frame Check Sequence* (FCS) ou *Cyclic Redundancy Check* (CRC).

A tabela abaixo mostra, teoricamente, entre outros detalhes, o tamanho da ocupação da banda em enlace FRF.12 aquando da aplicação da compressão e sem compressão, em virtude do tamanho de cabeçalho de cada protocolo conforme acima referido.

12.2.2.1.1 - Fórmulas dos resultados da tabela de cálculo de banda por compressão [3].

- ✓ **Codec Bit Rate (Kbps)** = codec sample size / codec sample interval;
- ✓ **Total packet size** = (L2 header: MP or FRF.12 or Ethernet) + (IP/UDP/RTP header) + (voice payload size);
- ✓ **PPS** = (codec bit rate) / (voice payload size);
- ✓ **Bandwidth** = total packet size * PPS.

12.2.2.1.2 - Demonstração do cálculo [3].

Por exemplo, a largura de banda de uma chamada usando o codecs G.729 (8 Kbps) com cRTP, MP e o payload default de voz é de 20 bytes. Eis o cálculo, então:

- ✓ **Total packet size (bytes)** = (MP header of 6 bytes) + (compressed IP/UDP/RTP header of 2 bytes) + (voice payload of 20 bytes) = 28 bytes;
- ✓ **Total packet size (bits)** = (28 bytes) * 8 bits per byte = 224 bits;
- ✓ **PPS** = (8 Kbps codec bit rate) / (160 bits) = 50 pps;
- ✓ **Bandwidth per call** = voice packet size (224 bits) * 50 pps = 11.2 Kbps;

✓ **Nota que:** 160 bits = 20 bytes (default voice payload) * 8 bits per byte;

Anteriormente detalhada, percebe-se a descrição detalhada do cálculo de tamanho de cabeçalho e consumo da largura da banda, conforme foi referido na introdução do capítulo anterior, tendo sido feitas as exposições necessárias sobre os codecs e cRTP. No capítulo XIII seguinte far-se-á considerações sobre a QoS. A QoS *diffServ* vai complementar de forma cabal todos os estudos e, na prática, ela diferenciar-se-á nos resultados das medições.

13 - CAPÍTULO XIII – CONSIDERAÇÕES SOBRE QoS

“A única coisa que dá vida à técnica é a qualidade intrínseca” – Silvani Severo

*“A tecnologia moderna é capaz de realizar a produção sem emprego.
O diabo é que a economia moderna não consegue inventar consumo sem salário” –
- Herbert de Souza*

13.1 – *Qualidade de Serviço (QoS) – Quality Of Service.*

Entende-se que a Qualidade de Serviço (QoS) deve ser conceituada como sendo um requisito fundamental das aplicações para a qual se exige que determinados parâmetros de avaliação de uma rede, tais como, perdas, atrasos, vazão, jitter, largura de banda, estejam dentro dos limites bem definidos. Essa exigência visa, por um lado, assegurar um contrato de prestação de serviço junto de um cliente e, por outro lado, prover garantias de bom funcionamento de uma rede, disponibilizando e reservando sempre a garantia de funcionamento eficiente e permanente da rede de acordo com o objetivo preconizado num dado momento. Desta forma, a técnica de QoS precisa garantir valores mínimos e máximos recomendados para os parâmetros de tráfegos anteriormente descritos, bem como prover garantia de recursos e serviço diferenciado ponto - a - ponto entre uma origem e um destino qualquer.

Na literatura, podemos encontrar o conceito de QoS expresso de uma forma simplificada: “Qualidade de Serviço (QoS) é um requisito da(s) aplicação(ões) para a qual exige-se que determinados parâmetros (atrasos, vazão, perdas, ...) estejam dentro de limites bem definidos (valor mínimo, valor máximo)” [49].

Desta forma, o QoS³⁷ constitui um desafio para o *backbone* de qualquer empresa bem-sucedida. Essas redes servem de transporte para uma série de aplicações, incluindo voz e vídeo com alta taxa de utilização de largura de banda. É fundamental o correto dimensionamento e configuração dos equipamentos que o compõem, para que tais aplicações possam funcionar conforme os níveis de serviços pretendidos.

As redes, portanto, devem fornecer serviços seguros, previsíveis, mensuráveis e às vezes garantidos a essas aplicações. Alcançar a qualidade de serviço exigida de ponta

37

‘A qualidade de serviço deve ser fim-a-fim, ou seja, considerando o modelo acima, o tráfego tem que ser tratado inicialmente na rede local (LAN) de origem, depois no próprio roteador (controle de descarte de pacotes, por exemplo), posteriormente nas conexões de longa distância (WAN) e roteadores intermediários, no roteador destino, e finalmente na rede local destino’ [62].

a ponta, mantendo ao mesmo tempo a simplicidade, a escalabilidade e a gerenciabilidade, é o segredo para executar uma infraestrutura que realmente atenda aos interesses das empresas de telecomunicações. Devido ao crescimento considerável da Internet nos últimos anos, abriu-se espaço para evolução de novas aplicações, impulsionando, assim, o surgimento de novos desafios tecnológicos que podem tornar o ambiente de comutação de circuito e tráfego de pacotes do tipo datagrama utilizado pela Internet propício às aplicações multimídia. É necessário, assim, a utilização de mecanismos de QoS para que os recursos de rede provejam o conforto e a satisfação do usuário.

13.1.1 - Visão Geral de QoS

A Internet iniciou-se com a ARPANET (*Advanced Research Projects Agency Network*), uma rede de dados experimental fundada pela DARPA (*Defense Advanced Research Projects Agency*), nos Estados Unidos nos anos 60. O objetivo principal era construir uma rede robusta e flexível que fosse capaz de sobreviver a ataques militares tais como bombardeios. Para alcançar esse objetivo, foi desenvolvido o modelo de datagrama, no qual cada pacote individual é encaminhado de forma independente na direção do seu destino. A rede Datagrama é robusta, simples e tem a habilidade de se adaptar automaticamente às mudanças da topologia da rede. Durante muitos anos a Internet foi utilizada por cientistas como uma rede de pesquisas e de troca de informações. O acesso remoto, a transferência de arquivos e a troca de e-mails foram, durante esses anos, as aplicações mais comuns. Esta rede é, atualmente, uma gigantesca rede pública. Novas aplicações como videoconferência, pesquisa, mídia eletrônica e telefonia pela Internet são uma realidade cada vez mais próxima e que está expandindo a uma velocidade sem precedentes. Podemos citar, como aplicação bem sucedida, o *E-commerce* que revolucionou a maneira de se fazer negócios [81]. A expansão e o sucesso da Internet motivaram o desenvolvimento de inúmeras aplicações com várias exigências, para as quais não foi originalmente projetada, ficando assim comprometido o seu desempenho.

O modelo datagrama no qual a Internet se baseia tem pouca capacidade de gerenciamento de recursos dentro da rede e não pode prover garantia de recursos para o usuário. Algumas aplicações como videoconferência, requerem recursos mínimos para uma operação efetiva. Coloca-se a questão dos serviços diferenciados. Como a Internet

trata todos os pacotes da mesma maneira, então só pode oferecer um único nível de serviço. Aplicações como telefonia sobre Internet são sensíveis à latência e perdas de pacotes. Em contrapartida, a transferência de arquivos pode tolerar atrasos sem a degradação de seu desempenho. O modelo de serviço tradicional oferece somente serviço de Melhor Esforço (*Best Effort*), que não dá nenhum tipo de garantia de que os pacotes enviados na rede chegarão ao seu destino. Este tipo de serviço não é adequado para tráfego sensível a atrasos, perdas de pacotes ou variações de atraso. Estas insuficiências podem diminuir a qualidade da transmissão em tempo real, podendo até inviabilizá-la [26].

A capacidade de prover garantia de recursos e serviços diferenciados é chamada de QoS. Com a introdução de QoS, pode-se reservar banda para tipos diferentes de fluxo de dados, onde os pacotes não são descartados e a banda não excede valores pré-definidos. Isto pode ser conseguido através da inclusão de controle de tráfego, alocação e gerência de recursos, policiamento, controle de admissão, entre outros. A QoS pode ser implementada de várias formas, como, por exemplo, a utilização de mecanismos de alocação de recursos; fazer uma otimização do desempenho ou ambos. A rede deve prover QoS baseado na solicitação da aplicação através do SLA³⁸ (*Service Level Agreement*). Os parâmetros negociados servem como referencial para que seja fornecida a qualidade solicitada. Entre os parâmetros mais comuns encontramos: vazão, atraso, jitter, perda de pacotes, taxa de erros e disponibilidade.

Existem duas arquiteturas de alocação de recursos dentro da Internet:

- ✓ Serviços Integrados
- ✓ Serviços Diferenciados

O MPLS possui mecanismo de provisão de TE que provê um conjunto de ferramentas de gerenciamento para provisionamento de banda e otimização do desempenho [48].

13.1.2 - Parâmetros que influenciam no planejamento de QoS.

O nível de QoS em uma rede é um parâmetro subjetivo, sendo mensurado a partir da monitoração de parâmetros específicos definidos no contrato de prestação de

38 SLA - Parte de contrato de serviços entre duas ou mais entidades no qual o nível da prestação de serviço é definido formalmente. Na prática, o termo é usado no contexto de tempo de entregas de um serviço ou de um desempenho específico. Por exemplo, se a empresa A contratar um nível de serviço de entregas de 95% em menos de 24 horas à Empresa B, esta já sabe que de todas as entregas que lhe forem dadas para fazer, no mínimo 95% tem que ser feitas em menos de 24 horas.

serviço estabelecido entre o provedor e o usuário. Os principais parâmetros que influenciam no planejamento de QoS são:

- ✓ Largura de Banda;
- ✓ Transparência Temporal e Transparência Semântica;
- ✓ Disponibilidade;

A Banda disponível na rede e a forma de compartilhamento desta largura para as diversas aplicações influenciam diretamente na QoS. A largura de banda é o parâmetro mais elementar para fornecimento da QoS. As aplicações geram vazões³⁹ que devem ser atendidas pela rede. As vazões para diversas aplicações são apresentadas na Tabela 47 a seguir [51].

Aplicações	Vazão
Aplicações Transacionais	1 kbps a 50 kbps
Quadro Branco (Whiteboard)	10 kbps a 100 kbps
Voz	10 kbps a 120 kbps
Aplicações Web (WWW)	10 kbps a 500 kbps
Transferência de Arquivos (Grandes)	10 kbps a 1 Mbps
Vídeo (Streaming)	100 kbps a 1 Mbps
Aplicação Conferência	500 kbps a 1 Mbps
Vídeo MPEG	1 Mbps a 10 Mbps
Aplicação Imagens Médicas	10 Mbps a 100 Mbps
Aplicação Realidade Virtual	80 Mbps a 150 Mbps

Tabela 47 - Vazão para diversas aplicações [51]

A Transparência Temporal corresponde ao atraso de pacotes e a variação do atraso denominado de Jitter. O atraso de pacotes é basicamente o intervalo de tempo entre o envio do pacote pelo transmissor e a recepção. O atraso tem um comportamento aleatório devido à intensidade do tráfego da rede. O Jitter é a variação do atraso gerado principalmente pela variação da carga da rede. O ideal seria ter atrasos pequenos e constantes. Uma forma de contornar este problema é utilizar um *buffer* na recepção que acrescente um atraso determinado, de forma a “nivelar” todos os atrasos. Os componentes de atraso podem ser fixos e/ou variáveis, existindo deste modo inúmeras formas de distinguir atrasos que são causados também por vários fatores distintos. em seguida enumeramos os distintos tipo de atraso:

³⁹ Deve-se tomar o cuidado para não se confundir a vazão (*throughput*) efetiva com a utilização do link. Uma rede com utilização alta não quer dizer que as informações estão sendo passadas com sucesso. Ela pode estar retransmitindo muito, pois a taxa de erro poder ser alta. O ideal é que uma rede com utilização alta, tenha uma vazão efetiva alta [51].

- ✓ **Atraso de propagação** – este atraso é fixo e representa o tempo que o sinal leva para se propagar no meio de transmissão, o que dependerá, portanto, do meio e da distância.
- ✓ **Atraso de codificação e decodificação** – este tipo de atraso é fixo e depende do algoritmo, tamanho do quadro e da capacidade de processamento.
- ✓ **Atraso de empacotamento** – é o tempo necessário para preencher o *payload* do pacote com os dados.
- ✓ **Atraso nos nós da rede** – o principal agente deste atraso é o enfileiramento nos roteadores, mais o tempo para decisão de roteamento e a transferência do buffer de entrada para o de saída.
- ✓ **Atraso devido ao Jitter do Buffer** – a variação do atraso da rede ocorre principalmente devido ao enfileiramento dos pacotes nos roteadores. Essa variação do atraso pode ser compensada por buffers. Entretanto, se ela for grande, pode ser inaceitável o atraso adicional para compensá-la.

A Transparência Semântica determina a possibilidade da rede transportar as informações livres de erro. O número de erros ponto-a-ponto introduzido pela rede tem que ser aceite por cada serviço fazendo com que cada aplicação demande de forma específica sua própria política e forma de planejar a QoS. Normalmente, quando se quer medir a taxa de erro de bits, mede-se no nível da transmissão (camada 1 do modelo OSI) e quando se quer medir a taxa de erro de pacote usa-se o nível da multiplexagem / comutação (camada 2 e 3 do modelo OSI) [52].

Devido à intolerância ao atraso, protocolos para transmissão confiável como TCP não podem ser utilizados tornando inevitável a perda. A perda de pacotes pode ocorrer devido a imperfeições na transmissão (problemas físicos, etc.) causando atraso que exceda o “*Time-to-Live*” e congestionamento que resulta em estouro de capacidade do *Buffer*. A disponibilidade seria medir o quão disponível estaria a utilização da rede para um determinado tipo de serviço. Geralmente, a disponibilidade é medida como uma porcentagem do dia, da semana ou do mês onde o recurso poderia ser usado, como 99,99%. Este parâmetro é fundamental para o funcionamento dos vários campos de negócio de empresas, principalmente se houver transações financeiras. Pode-se citar a disponibilidade das redes públicas e dos equipamentos presentes no caminho como fatores chave para uma QoS aceitável.

13.1.2.1 - Sensibilidade das aplicações

A sensibilidade para diversas aplicações é apresentada na Tabela 48 a seguir:

Tráfego	Sensibilidade			
	Largura de Banda	Perda	Atraso	Jitter
Voz	Muito baixo	Médio	Alto	Alto
Ecommerce	Baixo	Alto	Alto	Baixo
Transações	Baixo	Alto	Alto	Baixo
Email	Baixo	Alto	Baixo	Baixo
Telnet	Baixo	Alto	Médio	Baixo
Busca casual	Baixo	Médio	Médio	Baixo
Busca séria	Médio	Alto	Alto	Baixo
Transferência de arquivos	Alto	Médio	Baixo	Baixo
Vídeo conferência	Alto	Médio	Alto	Alto
Multicasting	Alto	Alto	Alto	Alto

Tabela 48 – Sensibilidade para diversas aplicações [52]

Essa sensibilidade é percebida através da predisposição das aplicações que podem ser classificadas em [26]:

- ✓ Aplicações multimídia.
- ✓ Aplicações tradicionais;
- ✓ Aplicações de missão crítica.

13.1.2.1.1 - Aplicações multimídia

Nas aplicações multimídias, além de mídias vídeos de *streams on demand*, encontram-se as aplicações de tempo real, como voz, videoconferência, telemedicina, ensino a distancia, entre outras. Assim, de forma comum se caracterizam as aplicações multimídias. Essas, entretanto, encontram-se divididas em três grandes classes de aplicações, a saber:

- 1 - Fluxo de áudio/vídeo armazenado (*Stored media; Streaming; Continuous playout*);
- 2 - Fluxo de áudio/vídeo ao vivo;
- 3 - Audio/vídeo interativos em tempo real.

Nas aplicações multimídia pequenas diferenças no tempo de entrega dos pacotes afetam sensivelmente os seus comportamentos. Nestas aplicações, a consistência das informações costuma ser menos importante do que a sua rápida transmissão. Sendo assim, durante a provisão desses serviços, as soluções de gerenciamento devem estar de acordo com às questões temporais e de QoS das redes de serviço [26].

13.1.2.1.2 - Aplicações tradicionais

As aplicações que demandam desses serviços de rede operam, normalmente, no modelo *best effort*, onde os conteúdos trafegam pela rede de acordo com a carga existente no momento do trânsito, não havendo qualquer tipo de garantia de entrega. A não garantia de entrega dessas aplicações é deve-se à inexistência de qualquer tipo de reserva de recursos na rede. Por causa disso, todas as informações são tratadas de forma igual e, perante esses congestionamento, as informações podem ser descartadas. As aplicações tradicionais costumam ser compostas por aplicações cujas características temporais não afetam a viabilidade e o comportamento das aplicações, a menos que haja perda. Podem ser enquadradas neste domínio algumas aplicações como aplicações de transferência de arquivos e emails, etc.

13.1.2.1.3 - Aplicações de missão crítica

Essas aplicações requerem um tratamento especial na rede fim-a-fim, devendo esta apresentar qualidades e garantias de serviços explícitos, principalmente com relação à entrega das informações. No leque dessas informações, o quesito tempo não é, necessariamente, muito importante para algumas das determinadas aplicações. A consistência, entretanto, dos dados é sempre importante. Como exemplo pode-se citar a realização de *backups* em sistemas distribuídos. O tempo total do *backup* é menos importante que a consistência dos dados copiados. Assim, durante a realização dos backups, todos os recursos da rede devem ser alocados a tal tarefa.

13.1.3 - Alocação de Recursos

Muitos problemas na Internet são resolvidos, fundamentalmente, com alocação de recursos. O atraso e a perda de pacotes decorrem da incapacidade de alocação de recursos ao longo da rede para atender a demanda de tráfego. Uma rede deve alocar recursos tais como largura de banda e *buffer* em função das características e requisitos da informação transportada. Uma rede com QoS tem condições de decidir quem deve utilizar os recursos, quando e quanto. A Internet convencional trata cada pacote individualmente e da mesma maneira, utilizando a disciplina FIFO (*First In First Out*). Não existe, portanto, um controle de admissão se o usuário desejar injetar pacotes tão rápidos quando for possível. A Internet convencional trabalha com o protocolo TCP nos hospedeiros para detectar congestionamento na rede e reduzir a taxa de transmissão de acordo com a ocasião. O TCP usa um esquema baseado em janela para controle de congestionamento. A janela corresponde à quantidade de dados que pode ser transmitida

do transmissor para o receptor. Se a fonte TCP detectar perda de pacotes, a taxa de transmissão será reduzida, diminuindo, assim, o tamanho da janela pela metade e aumentando gradativamente, se houver largura de banda disponível. Este mecanismo é eficaz em um grupo pequeno. Contudo, para a Internet que tem dimensões extremamente grandes, isso torna-se impraticável.

O serviço *Melhor Esforço* é o serviço mais simples que a rede pode oferecer e não apresenta nenhuma forma de assegurar recursos para o tráfego. Quando um enlace está congestionado, os pacotes que chegam excedem a capacidade do buffer. Por isso, este método é passível de congestionamento. Desse modo, o serviço *Melhor Esforço* é tolerável para aplicações de transferência de arquivos e e-mails e não satisfaz as necessidades das novas aplicações multimídia. Os serviços Integrados (*IntServ*) e os Serviços Diferenciados (*DiffServ*) constituem duas soluções diferentes para contornar tais situações. O *IntServ* provê garantia de recursos através da reserva desses recursos para fluxos de aplicação individual, enquanto que o *DiffServ* usa a combinação entre policiamento avançado, provisionamento e priorização de tráfego, para prover QoS em uma rede, diferenciando grandemente dos serviços *Melhor Esforço* da rede [51],[56].

13.1.3.1 - Serviços Diferenciados – *DiffServ*.

A filosofia de funcionamento dos algoritmos de QoS para serviço diferenciado baseia-se, basicamente, na premissa de que “a qualidade de serviço pode ser garantida através de um mecanismo de priorização de pacotes na rede” [51]. O *DiffServ*, conforme a ilustração abaixo, foi introduzido devido à grande dificuldade de implementação e desenvolvimento do *Intserv*. Com o *DiffServ*, pretende-se obter a escalabilidade através da agregação de fluxos em grandes conjuntos BA (Behavior Aggregate), provisionamento de recursos para essas agregações (sem protocolos de reserva) e separação das funções dos roteadores de núcleo e borda. Apesar de ser escalável, o *DiffServ* não oferece a garantia de recursos para todos os fluxos como oferece o *IntServ*. As reservas de recursos são feitas para agregações e um fluxo individual pode não atingir suas necessidades em termos dos parâmetros de QoS. A priorização pode ser feita, por exemplo, no IPv4, através do campo TOS (*Type Of Service*) de seu cabeçalho e no IPv6, através do campo *Traffic Class*. Obtêm assim as Classes de Serviço. Os roteadores ordenam os pacotes de entrada em diferentes classes

de encaminhamento, de acordo com os valores correspondentes de *DS Field*. **Existem dois tipos de classificação** dentro do *DiffServ*:

- ✓ BA (*Behavior Aggregate*), é baseada somente no campo DSCP (*Diffserv Code-Point*) e,
- ✓ MF (*Multi-field*), baseada em endereço do destino, endereço da fonte, número da porta e a classificação do campo DS.

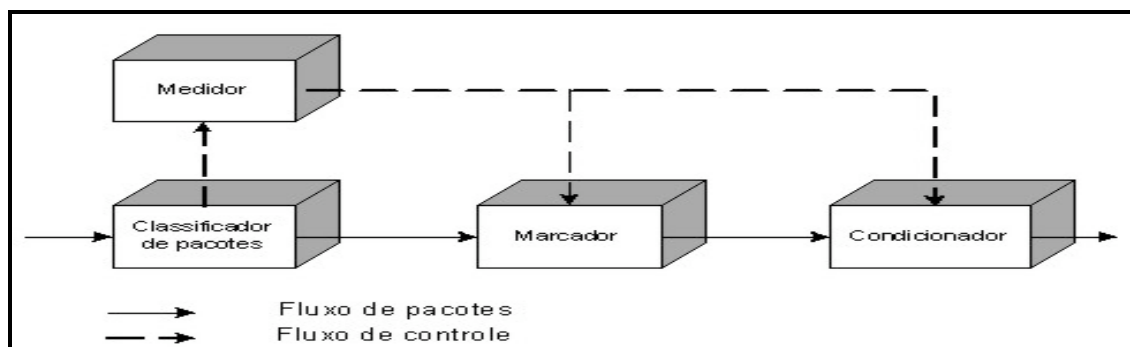


Figura 66 - Arquitetura funcional do *DiffServ* [51]

De acordo com a Figura 66 em apreço, vale acrescentar que a classificação MF permite a separação do tráfego direcionado para uma determinada classe de serviço e realizar também a marcação do campo DSCP com o valor apropriado. Já o classificador (BA) é utilizado pelos nós da rede admitindo que os fluxos encontram-se definidos e os pacotes devidamente marcados. Deste modo, o processo de classificação torna-se, consideravelmente, simples e rápido.

13.1.3.1.1 - Descrição dos parâmetros de fluxo da arquitetura funcional do *DiffServ*:

Conforme a Figura 66, os fluxos de pacotes e os fluxos de controle têm as seguintes funcionalidades:

- ✓ **O medidor** verifica a taxa de transmissão de tráfego a qual este está submetido e compara com os parâmetros que estão armazenados em um determinado perfil. Como uma forma simples de policiamento de tráfego, posteriormente, deve se concluir através de uma análise que informa se o tráfego está ou não de acordo com o perfil;
- ✓ **O marcador** é utilizado para colocar um valor específico no campo DSCP (*Differentiated Services Code Point*);

- ✓ **O condicionador** como uma forma de policiamento, altera a característica do tráfego que foi submetido através da inserção de atraso de pacotes.
- ✓ **O descartador** descarta pacotes que não estão em conformidade com alguma regra de policiamento. Os nós de rede, individualmente, realizam o processamento do pacote com base no campo *DSCP*. Assim, o modelo implementa o conceito de comportamento por salto PHB - *Per Hop Behavior*, implementando, deste modo, cada nó o modelo DiffServ resultando em um comportamento bem definido e padronizado. Alguns dos modelos de padronização de conjuntos de PHB muito utilizados na marcação de pacotes são : EF (*Expedited Forwarding*) e o AF (*Assured Forwarding*) com as suas respectivas variações numéricas, segundo o IETF [51],[19].

Conforme a especificação RFC 2598 [19] o PHB EF pode ser usado para um serviço fim-a-fim com baixas margens de latência, baixa perda de pacotes e atraso também baixo, porém, com banda assegurada, para os serviços de conexões ponto-a-ponto e, ou com uma linha virtual dedicada, por essa natureza, é descrito também como *Premium Service*. A implementação de um PHB EF inclui, necessariamente, algum mecanismo que evite que o tráfego EF afete de uma forma ou outra qualquer outro tráfego. Os escalonadores de pacotes também podem ser empregados para suportar o PHB EF. Contudo, para se criar um serviço EF precisam-se implementar dois passos significativos:

- ✓ Configurar os nós para que os fluxos agregados tenham taxa de encaminhamento mínima;
- ✓ Condicionar as agregações via policiamento, para que a taxa de chegada nos nós seja sempre menor que a taxa mínima de encaminhamento configurada no nó.

Com relação ao mecanismo de PHB AF - chamado grupo de encaminhamento assegurado - mais considerações são obtidas através da referência RFC 2597 [58]. Este mecanismo proporciona diversos níveis de encaminhamento de pacotes IP, desde que o tráfego agregado não estaria o limite do perfil de tráfego declarado ou contratado. Partindo desse pressuposto, verifica-se que existem quatro classes AF, que são definidas em cada um dos nós, reservando espaço em buffer e largura de banda. Para cada classe AF todavia existem, três valores que indicam a probabilidade de ocorrer um descarte do

pacote, pelo que sempre que houver congestionamento o descarte é feito, levando em conta a classe e a probabilidade de descarte escolhidos.

No PHB AF o controle de tráfego é feito na borda, podendo descartar, convenientemente, pacotes, diminuir ou aumentar a probabilidade de descarte e remarcação dos pacotes para outras classes AF. Pois, o PHB AF, não garante requisitos de tempo como *jitter* e atraso[58]. O *DiffServ* parte do princípio de que domínios adjacentes têm acordo sobre os serviços disponibilizados. As operações de classificação, policiamento e condicionamento são necessárias somente nos limites da rede (bordas). No centro da rede, os roteadores classificam e encaminham os pacotes. Os pacotes poderão receber tratamentos distintos em função da QoS que necessitarem. Esses tratamentos de encaminhamento são chamados de PHB (*Per-Hop-Behavior*). O PHB é o modo como um roteador central aloca recursos para os Bases e é, com base, nesse mecanismo local que serviços são construídos. A maneira mais simples de implementar um PHB é destinar-lhe uma determinada percentagem de utilização da banda de um enlace de saída [51].

13.1.3.1.2 - Os grupos de PHBs padronizados são:

- ✓ **AF (*Assured Forward*):** para aquelas aplicações que necessitam de uma confiabilidade maior do que o serviço de Melhor Esforço, embora não garanta qualquer limite para atraso e jitter. O nó deve alocar uma quantidade de buffer e banda para cada classe e fila para os pacotes AQ (***Assured Queue***), gerenciada por um esquema chamado RED (***Random Early Drop***) para evitar congestionamento. Se uma AQ for substituída por outras três filas, gerenciadas pelo algoritmo WFQ, poderão ser oferecidos serviços de encaminhamento diferentes (serviços ouro, prata e bronze).
- ✓ **EF (*Express Forward*):** para aplicações que necessitam de pouco atraso, jitter e taxa de perda, além de garantia de banda. É chamado de “linha privada virtual” ou serviço *premium*. (Ex: telefonia via Internet, videoconferência, etc.). As filas na interface de saída devem permanecer descongestionadas, sendo a taxa de saída dos pacotes do nó maior que a taxa de entrada. Os pacotes entrarão em filas Premium (PQ) para serem enviados, podendo utilizar políticas de escalonamento de filas como o WFQ, WRR (***Weighted Round Robin***) e CBQ (***Class-based Queuing***).

- ✓ **CSC (Class Selector Compliant):** grupo criado com o objetivo de manter a compatibilidade com as implementações existentes de IP *Precedence*, um padrão antigo para especificação de pacotes IP. Além desses grupos, um PHB *default*, ou PHB BE (*Best Effort*) foi definido para encaminhamento de tráfego de Melhor Esforço. As regras de classificação, policiamento, condicionamento e escalonamento, usadas nos roteadores são determinadas pelo SLA tanto quanto o espaço nos *buffers* de cada roteador.

Um SLA determina quais classes de serviços são suportadas e a quantidade de tráfego na banda entre os domínios. No *DiffServ* o SLA pode ser estático ou dinâmico. O SLA estático está associado ao AF; já no EF é desejável que o provedor suporte SLAs estático e dinâmico. O esquema de controle de admissão para suportar SLAs dinâmicos é conhecido como BB (*Bandwidth Broker*). O BB autoriza ou não a entrada de determinado tráfego em seu domínio e sinaliza para BB de outros domínios através dos quais o fluxo irá atravessar [51]. Dessa forma, conclui-se que o *DiffServ* apresenta desvantagem em relação a alguns serviços diferenciados, dando, contudo, segurança ao desempenho das aplicações somente em termos relativos, garantindo que uma aplicação gerando tráfego de determinada prioridade venha a ter melhor desempenho que outra gerando tráfego de menor prioridade. Surge, nesse aspecto, técnicas de enfileiramento de QoS provendo controle e inibição de congestionamento, o que proporciona de forma explícita a otimização de desempenho em redes. Surgem, deste modo, vários mecanismos e técnicas de enfileiramento para controle e prevenção de congestionamento em interfaces de roteadores (Ethernet, seriais, Frame Relay, MPLS, etc.) e switches nível 3 (L3), aplicáveis tanto em redes WAN (*Wide Area Network*) como em LAN. A seguir ao item otimização de desempenho as principais técnicas serão apresentadas [62].

13.2 - Especificação da implementação de CoS - filas de QoS em roteadores Cisco

A rede de pacotes da OP é uma rede de dados que precisa de fornecer interface de comunicação para a rede da operação interna da OP assim como prover interfaces para serviços externo a OP. Essa rede deve prover serviços gerenciais e de procedimentos correntes entre os funcionários como intranet e internet, telefonia, etc..., e interfaces de testes de viabilidade dos equipamentos às aplicações antes que sejam em definitivo colocados, comercialmente, em operação. Esta mesma rede provê, ainda,

serviços de telecomunicações e permite conexão com o backbone da OP e as demais conexões externas pelo Brasil e pelo mundo. Esta rede de pacote precisa de ser robusta o suficiente para, além de prover interface de acesso aos serviços, ser, também, uma rede tal que comporta eficientemente requisitos de QoS, projetados e implementados a fim de garantir confiabilidade, escalabilidade, requisito de tempo. Posto isso, a rede estará em condições de funcionar de forma operacional. Decorrente disso, esta seção especifica a metodologia de implementação de CoS e filas de QoS adotadas pelos equipamentos de comutação (routers) da OP e que foram utilizados durante os testes. Alguns desses equipamentos foram disponibilizados pela OP para compor a topologia física da Mini-rede de pacotes usado para medições. Esse levantamento permite efetuar a análise da forma de mapeamentos de classes de serviços – QoS e formas de policiamento de tráfego e a filosofia de mapeamento e suporte a algoritmos de enfileiramento de tráfego. Os equipamentos disponíveis são da *Cisco Routers*, serie-2600, 1751v e, 1760. Estes equipamentos fazem parte dos nós de acesso ao backbone da mini-Rede CRT IP VPN / MPLS Multicasting. Esta seção não diz respeito à especificação dos equipamentos, mas sim exclusivamente às formas de provisão de QoS *diffserv*, pois durante todos os testes e medições foram implementadas essas políticas.

13.2.1 - Do mapeamento de Classes de Serviços (CoS):

Estes equipamentos de acesso mapeiam e implementam 8 (oito) filas diferentes para oito classes de tráfegos de serviços (*DiffServ*) bem definidas, conforme ilustra a Tabela 49 a seguir.

CoS (bits)	CoS (in Decimal)	Definition	Application
000	0	Routine	Best-effort data
001	1	Priority	Medium-priority data
010	2	Immediate	High-priority data
011	3	Flash	Call signaling
100	4	Flash-Override	Video conferencing
101	5	Critical	Voice bearer
110	6	Internet	Reserved (inter-network control)
111	7	Network	Reserved (network control)

Tabela 49- Definições das CoS suportadas pelos equipamentos comutação Cisco [27].

Percebe-se, então, que temos um conjunto de aplicações variadas e com propriedades diferentes entre si e que facilmente nos dá margem de poder agregar tráfegos em classes para posterior marcação de prioridades. Essas aplicações, por outro lado, são dotadas de definições específicas que determinam com precisão os níveis de

criticidade que as mesmas classes devem pertencer. Entende-se, por definição, que a classe que deve compor o valor CoS = 2 merece atenção particular, já que à esta classe são agregadas as aplicações de dados de alta prioridade, merecendo, deste modo, uma definição de marcação de tratamento imediato na fila.

13.2.1.1 - Classes de serviço da AutoQoS

O Cisco por padrão implementa a AutoQoS que é composta por dez (10) tipos de CoS, conforme a Tabela 50 a seguir.

Class Name	Traffic Type	DSCP Value	CoS Value
IP Routing	Network control traffic such as routing protocols	CS6	6
Interactive Voice	Interactive voice bearer traffic	EF	5
Interactive Video	Interactive video data traffic	AF41	4
Streaming Video	Streaming media traffic	CS4	4
Telephony Signaling	Telephony signaling and control traffic	CS3	3
Transactional and Interactive	Database applications that are transactional in nature	AF21	2
Network Management	Network management traffic	CS2	2
Bulk Data	Bulk data transfers, web traffic, general data service	AF11	1
Scavenger	Entertainment, rogue traffic, and less than best-effort traffic	CS1	1
Best Effort	All noncritical and miscellaneous traffic	BE	0

Tabela 50 - Classes de tráfego definidas pela AutoQoS [27].

A AutoQoS permite os mecanismos LLQ (*Low-latency queuing*) de enfileiramento e WRR - necessários para assegurar uma boa qualidade de voz e vídeo em uma banda durante o congestionamento. O tráfego de voz é tratado como *DiffServ EF* com a maior prioridade e é colocado em uma fila de prioridade estrita com banda garantida e policiada. O tráfego de dados da sinalização e da empresa é tratado como classes de *DiffServ AF* e CBWFQ é utilizado por essas classes, dando a cada classe uma fila separada com garantias mínimas da largura de faixa. O tráfego não classificado é tratado como *DiffServ BE* e é atribuído à classe *default*. A alocação da largura de banda é feita usando uma percentagem da largura de banda do link por razões de melhores escalabilidade e viabilidade. Porém em Switches LAN, WRR é utilizado com uma fila de prioridade para o tráfego *real-time*.

O *DiffServ* permite a implementação de modelos de marcação de pacotes através da técnica *Differentiated Services Code Point (DSCP) - Per-Hop Behavior (PHB)*, permitindo, contrariamente ao *IntServ* que usa o *IP Precedence*, o uso do campo ToS = 8bits de cabeçalho IP. Para garantir a alta probabilidade de encaminhamento de pacotes em tempo hábil, o *DiffServ* usa uma técnica similar ao ToS, o campo DSCP - PHB de 6 bits. Este campo é usado para controle de fluxo e tem a chamada dos bits *Explicit*

Congestion Notification (ECN) para mapear e marca os serviços através do comportamento (PHB) e perfil de tráfego após a sua devida classificação em grupos. Assim, o campo DSCP do cabeçalho IP determina para o *DiffServ* quatro tipos diferentes de marcação: **Default PHB** (Usado para serviços melhor esforço; **Class selector PHB** (Usado em compatibilidade para os serviços não DiffServ. O CS-PHB (CS1 a CS7-mais significativa) fornece a compatibilidade inversa à precedência baseada ToS do IP.); **Assured forwarding (AF) PHB** e, **Expedited forwarding (EF) PHB**.

13.2.1.1.1 - Assured forwarding (AF) PHB

Usado para serviços que precisam de banda garantida. AF PHB fornece quatro filas para quatro classes de tráfego tipo AFxy. Para cada fila é reservada uma largura de banda pré-especificada. Se a quantidade de tráfego em uma fila particular exceder a largura da banda reservada para essa fila, a mesma acumulará e, eventualmente, ocorrerá perda de pacote.

<i>The AF DSCP Values</i>			
Class	Drop Probability		
	Low Drop	Medium Drop	High Drop
Class 1	AF11	AF12	AF13
	DSCP 10: (001010)	DSCP 12: (001100)	DSCP 14: (001110)
Class 2	AF21	AF22	AF23
	DSCP 18: (010010)	DSCP 20: (010100)	DSCP 22: (010110)
Class 3	AF31	AF32	AF33
	DSCP 26: (011010)	DSCP 28: (011100)	DSCP 30: (011110)
Class 4	AF41	AF42	AF43
	DSCP 34: (100010)	DSCP 36: (100100)	DSCP 38: (100110)

Tabela 51 – Filas-Classes AF PHB - DSCP, probabilidade de descarte de pacotes [27]

De acordo com a Tabela 51, para evitar perda, congestionamento, técnicas como *Weighted Random Early Detection* (WRED) são implementadas em cada fila. A representação numérica decimal indica que os números maiores não são melhores; indica, igualmente, uma preferência mais elevada de probabilidade de perda. A tabela abaixo representa as filas e a probabilidade de maior perda para cada classe [27],[28].

13.2.1.1.2 - Expedited forwarding (EF) PHB

Usado para serviços de baixo delay, devendo minimizar o jitter e a perda. É adequado aos serviços de voz, vídeo e outros de tempo real e a fila adequada é a *priority queue* dedicada de alta prioridade; a largura de banda dedicada a EF deve também ser

limitada de modo que outras classes do tráfego não fiquem sem faixa de banda. A *EF* impõe, assim, largura de banda mínima (não em redes típicas é limitada a banda para tráfego *EF* a não mais de 30% da capacidade de enlace), banda garantida e durante gargalos de congestionamentos ela serve para policiar a banda [28]. Apontamos a seguir algumas considerações a respeito das políticas de QoS.

13.2.2 - Implementação e verificação de AutoQoS.

A AutoQoS permite habilitar funções de *diffserv* nas interfaces dos equipamentos, para uma variada tecnologia de acesso, como o Frame Relay e suas funções específicas, conforme a tabela que se segue. Entretanto, a AutoQoS, deve ser habilitada para determinadas interfaces e PVC apenas. As interfaces que podem ser habilitadas AutoQoS são:

- ✓ Interfaces Serial com PPP ou encapsulamento HDLC (*high-level data link control*);
- ✓ Sub-interfaces Frame Relay point-to-point e jamais Multipoint;
- ✓ Sub-interfaces ATM point-to-point (PVCs) inclusive em baixa capacidade (≤ 768 kbps) e interfaces *Fast Serial* (> 768 kbps);
- ✓ Links de *interworking* Frame Relay-to-ATM.

Em link serial de baixa velocidade a AutoQoS é habilitada em ambas as pontas e a configuração da banda deve ser consistente. Para encapsulamento PPP e *Multilink* PPP (MLP) é habilitada automaticamente em endereços IP das interfaces Seriais e é removido e colocado em uma MLP virtual. Em link Frame Relay (rede de tráfego tipo rajada) esta deve ser habilitada nas interfaces de endereço lógico diferente de acesso remoto - DLCI (*Data-Link Connection Identifier*) levando em conta os devidos cuidados e restrições ao configurar e gerencia a banda. O mau conhecimento dos parâmetros como (CAR - *Committed Access Rate*, CIR - *Committed Information Rate*, etc, da modalidade FRTS (*Frame Relay Traffic Shaping*) atrapalha o bom funcionamento do tráfego, ao invés de surtir efeito desejado [27].

DiffServ Function	Cisco IOS QoS Feature That AutoQoS Uses
Classification	Using NBAR (on untrusted links)
	Using IP precedence, DSCP, or CoS (trusted)
Marking	Class-based marking
Congestion management	LLQ (Strict PQ + CBWFQ) using percentage BW
	WRR (on Catalyst LAN switches)
Shaping	CBTS ¹
	FRTS ²
Congestion avoidance	WRED ³
Link efficiency	LFI
	MLP
	cRTP

¹ CBTS = class-based traffic shaping
² FRTS = Frame Relay traffic shaping
³ WRED = weighted random early detection

Tabela 52 - Funções *DiffServ* - recursos da Cisco para habilitar a AutoQoS [27].

Ao habilitar a AutoQoS (Tabela 52) alguns recursos, como os que estão discriminados abaixo, podem permitir, ser de forma eficiente, habilitados nas interfaces dos roteadores:

LLQ (*Low Latency Queuing*) – Reserva uma fila com prioridade para tráfego de VoIP (*Voice Over Internet Protocol*) (RTP) com banda garantida e com policiamento. Reserva, também, filas CBWFQ - (*class-based weighted fair queueing*) para tráfegos de Missão - crítica transacional e tráfegos de sinalização todos com garantias da largura de banda.

RTP (*Compressed RTP (Real Time Protocol)*) ao habilitar consegue, portanto, reduzir o cabeçalho de IP/UDP/RTP de 40 bytes a 2/4 dos bytes. Esta característica costuma ser habilitada nas interfaces seriais de baixa velocidade.

LFI (*Link Fragmentation and Interleaving*) Intercalam os pacotes de dados de fragmentos grandes em relação aos pacotes pequenos com os quadros de voz. Isso acontece em filas compartilhadas, evitando que os pacotes grandes tipo FTP atrapalhem o tráfego de voz que não pode ser fragmentado.

A AutoQoS serve ainda para habilitar a FRTS onde for necessário. FRTS é especialmente importante por duas razões: a taxa de *clock* de disparo da interface (velocidade física) é geralmente mais elevada do que a taxa CIR. Daí a necessidade da configuração correta da largura da banda em interfaces seriais e nas sub-interfaces antes da ativação de AutoQoS nas respectivas interfaces. Os sites de uma empresa são, geralmente, conectados em uma topologia interconectados por *hub* e os fluxos de tráfego de um ou muitos sites podem causar congestionamento e a perda dos dados para os sites de destino. Assim, para evitar tais congestionamentos é usada a WRED em área de gargalo da rede, habilitando as funções da AutoQoS [27],[28].

13.2.3 - Definindo políticas para cada classe de tráfego.

Depois da formação das classes de tráfego, deve ser definido para toda a rede o nível de serviço de QoS que deve ser atribuído a cada classe de tráfego. Atribui-se a essa medida o nome de política de QoS que inclui determinar as seguintes tarefas:

- ✓ Ajustar o limite máximo da largura de banda para uma classe;
- ✓ Ajustar uma garantia mínima da largura de banda para uma classe;
- ✓ Atribuir um nível de prioridade relativo a uma classe;
- ✓ Aplicar a gerência de congestionamento, contenção de congestão e muitas outras técnicas avançadas de QoS associadas a uma classe.

Para ilustrar algumas políticas praticadas pelos equipamentos ciscos, a Tabela 53 a seguir exemplifica a prática comum para a QoS para alguns dos principais serviços [27].

Class	Priority	Queue Type	Min/Max Bandwidth	Special QoS Technology
Voice	5	Priority	1 Mbps Min 1 Mbps Max	Priority queue
Business mission critical	4	CBWFQ	1 Mbps Min	CBWFQ
Signaling	3	CBWFQ	400 Kbps Min	CBWFQ
Transactional	2	CBWFQ	1 Mbps Min	CBWFQ
Best-effort	1	CBWFQ	500 Kbps Max	CBWFQ CB-Policing
Scavenger	0	CBWFQ	Max 100 Kbps	CBWFQ +CB-Policing WRED

Tabela 53 - Definição de políticas de QoS para as Classes de Tráfego de serviços [27].

Pode-se perceber que para a Tabela 53, para cada aplicação pertencente à classe de serviço é recomendada uma tecnologia de QoS especial para a fila, neste caso o CBWFQ - (*class-based weighted fair queueing*), com nível de prioridades para cada classe e a parte crucial, disto tudo e a recomendação da garantia de banda passante para cada aplicação, com a capacidade mínima e a capacidade máxima recomendada, sendo que a reserva de banda abaixo do mínimo aconselhado, para cada classe, as aplicação que dela derivam ficariam sujeitas a descarte de pacotes. De forma mais visível, no cotidiano os nomes de aplicações comerciais comumente conhecidos para os tráfegos entre os provedores e os clientes, são:

- ✓ Aplicações da voz do (VoIP);
- ✓ Aplicações de Missão Crítica tais como Base de dados Oracle;

- ✓ Aplicações Transacional / interativas, tais como o *telnet* e o *SSH*;
- ✓ Aplicações FTP e o TFTP;
- ✓ Aplicações Melhor-esforço tais como WWW e Aplicações de email;
- ✓ Acesso a aplicações como *Napster* e *Kazaa*.

Uma das tarefas exigidas durante o estágio de execução da política de QoS é a de mapear e traduzir a CoS, bits de precedência de DSCP e IP e as marcações de MPLS EXP (Campo experimental usado na marcação de frames de cabeçalho MPLS de 3 bits).

13.2.4 – Disciplinas de Escalonamento para Otimização de Desempenho.

Uma vez escolhidos a arquitetura de alocação de recursos e os modelos de serviços, a segunda questão é a otimização do desempenho, isto é, como organizar os recursos numa rede de modo mais eficiente para maximizar a probabilidade de entrega dos pacotes e minimizar o custo de entrega. A conexão entre a otimização do desempenho e o suporte a QoS pode parecer menos direta comparada com a alocação de recursos. A otimização do desempenho é, no entanto, um importante bloco de construção no desenvolvimento de QoS *DiffServ*.

O roteamento baseado em datagramas da Internet não foi projetado para otimizar o desempenho da rede. Escalabilidade e manutenção da conectividade em face das falhas foram os objetivos primários do projeto. Os protocolos de roteamento, basicamente, escolhem o menor caminho até o destino, baseado em algumas métricas simples, como contagem de saltos ou atraso. Mecanismos tão simples, claramente, não são adequados para o suporte a alocação de recursos. Por exemplo, para se fazer uma reserva é preciso encontrar um caminho com certos requisitos de recursos, como largura de banda, mas o roteamento IP não tem a informação necessária para tomar tais decisões. Usar apenas o algoritmo de menor caminho para selecionar rotas, provavelmente, causará uma alta taxa de rejeição. O roteamento de menor caminho nem sempre usa as diversas conexões disponíveis na rede.

Na verdade, o tráfego é freqüentemente distribuído, de forma desigual, pela rede o que pode criar pontos de congestionamento enquanto que outras partes da rede podem estar muito pouco carregadas [48].

A otimização do desempenho requer capacidades adicionais no roteamento IP e ferramentas de gerenciamento do desempenho. Para gerenciar o desempenho de uma

rede, é necessário ter um controle explícito sobre os caminhos e o tráfego de modo que os fluxos possam ser organizados para maximizar os recursos e a utilização da rede. O MPLS tem um mecanismo chamado roteamento explícito que é ideal para esse propósito.

O MPLS usa a abordagem de comutação de rótulos para estabelecer circuitos virtuais em redes baseadas em IP. Esses circuitos virtuais podem seguir o roteamento IP baseado no destino, mas o roteamento explícito no MPLS também nos permite especificar salto a salto todo o caminho desses circuitos virtuais. Isso provê um modo de ignorar o roteamento baseado em destino e estabelecer troncos de tráfego baseados em objetivos de Engenharia de Tráfego.

O processo de otimização do desempenho das redes através de provisionamento eficiente e melhor controle dos fluxos é geralmente chamado de Engenharia de Tráfego. A Engenharia de Tráfego usa algoritmos avançados de seleção de rotas para abastecer os troncos de tráfego dentro de backbones e organiza os fluxos de tráfego de forma a maximizar a eficiência global da rede.

A abordagem comum é calcular os troncos de tráfego baseado na distribuição do fluxo e então estabelecer os troncos como rotas explícitas com o protocolo MPLS. A combinação do MPLS com a Engenharia de Tráfego provê redes IP com um conjunto de ferramentas avançadas para que os provedores de serviço gerenciem o desempenho de suas redes e tenham capacidade para prover mais serviços a um custo menor.

13.2.4.1 - Disciplina FIFO (*First In First Out*)

A disciplina de escalonamento do tipo “FIFO” é a mais elementar de todas. Todos os pacotes são tratados iguais; são colocados em uma única fila e servidos na mesma ordem da sua chegada, conforme esquematiza a Figura 67 a seguir. Esta disciplina também é conhecida como FCFS (*First Come First Served*) [53],[62].

A disciplina do tipo FIFO, apesar de ser a mais elementar operação de escalonamento, oferece algumas vantagens, assim como apresenta algumas desvantagens que são peculiares em determinadas técnicas. Passo a indicar algumas das desvantagens:

- ✓ Carga computacional extremamente baixa se comparada com outras disciplinas;
- ✓ Comportamento previsível;

- ✓ Atraso é determinado pelo tamanho da fila.

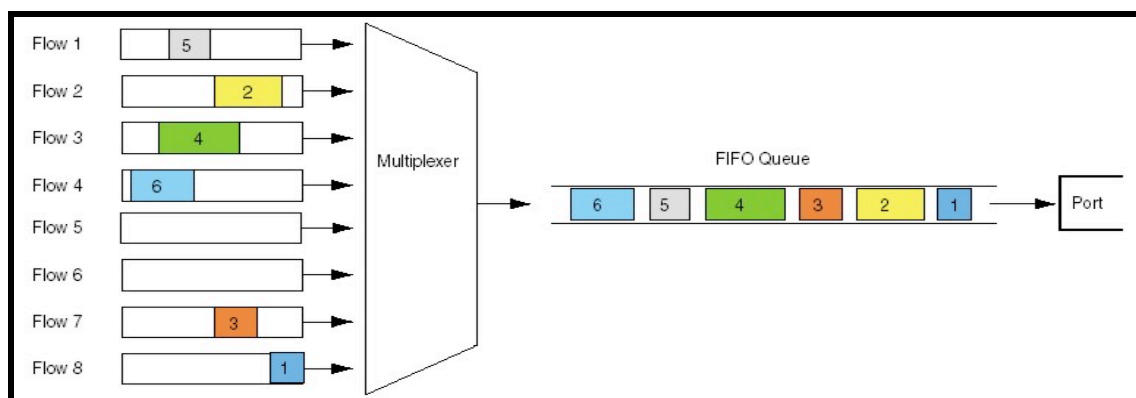


Figura 67 - Escalonamento FIFO [53]

Em contrapartida, verificam-se também algumas limitações de um algoritmo de escalonamento, das quais destacamos as seguintes:

- ✓ Uma única fila FIFO não permite reordenar/organizar os pacotes armazenados sendo incapaz de priorizar classes de tráfego;
- ✓ Uma única fila FIFO trata igualmente todos os fluxos. Assim, o atraso aumenta da mesma forma para todos os fluxos à medida que ocorre um congestionamento. Como resultado, FIFO pode significar atraso, jitter e perda para aplicações de tempo real;
- ✓ Durante um congestionamento, a FIFO beneficia fluxos de UDP sobre fluxos de TCP. Quando ocorre perda de pacote durante o congestionamento, as aplicações baseadas em TCP reduzem suas taxas de transmissão, mas aplicações baseadas em UDP permanecem constantes. Assim, o uso da FIFO pode resultar em aumento de atraso, jitter e redução da largura da banda consumida pelas aplicações TCP;
- ✓ Um fluxo de rajada pode consumir toda a fila e prejudicar os outros fluxos.

13.2.4.2 - Disciplina PQ (*Priority Queuing*)

PQ é a base para uma disciplina de escalonamento que suporte classes de serviço diferenciadas. Na PQ clássica, os pacotes são classificados primeiro pelo classificador e são colocados em filas (FIFO) de prioridade diferentes (vide figura abaixo). Os pacotes apenas são retirados de uma determinada fila se as filas de prioridades mais altas estiverem vazias [53]. Não existe, assim, uma fila específica para determinada classe ou tipo de tráfego. Dessa forma, pode-se considerar esse método como uma maneira

clássica e simples de prover tráfegos com determinada diferenciação, uma vez que foi projetado para dar a todos os programas de alta prioridade, os ditos programas de missão crítica prioridades sem precedentes em comparação aos tráfegos menos críticos, ou seja, tráfegos menos importantes. Adotando esta técnica, quando ocorrem ciclos de gargalos de tráfegos, estes tráfegos congestionados são então enfileirados como alta, normal, média ou até baixa. Vide a Figura 68 a seguir. Figura 68 exemplifica essa ideia.

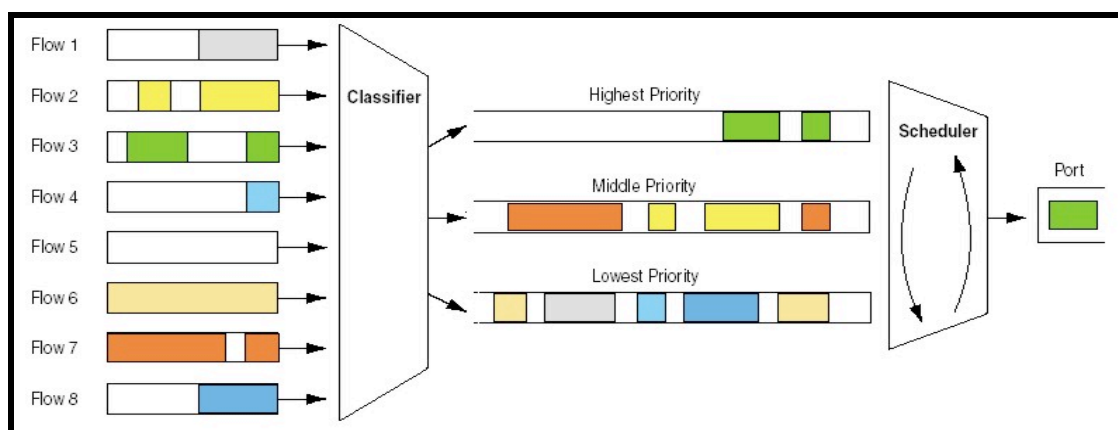


Figura 68 - Técnica enfileiramento PQ [53]

Usando, portanto, o PQ, todo tráfego de alta prioridade é atendido primeiro, em seguida, o tráfego normal e assim por diante [54]. Esta técnica de escalonamento de enfileiramento⁴⁰ em comparação ao FIFO possui também as suas vantagens e desvantagens, conforme abaixo se pode verificar. Se existirem muitos fluxos de alta prioridade, todos os recursos serão destinados a eles e as filas de menor prioridade não terão recursos disponíveis para encaminhar os pacotes. Este efeito é chamado de *starvation* (paralisação), derivada normalmente de uma alocação injusta, de recurso da fila.

Starvation ocorre também, quando há, por exemplo, atribuição de prioridade às aplicações cujas funcionalidades de requisitos de tempo real não são críticas em uma fila com aplicações cujos requisitos de tempos são críticos, com tempo de execução bem determina. Essa atribuição indevida de prioridade de escalonamento também pode provocar o fenômeno *Starvation* [63],[64]. **Esta disciplina do tipo PQ oferece as seguintes vantagens:**

- ✓ Carga computacional relativamente baixa se comparada com outras disciplinas;

40

Enfileiramento é uma técnica usada na interconexão de dispositivos de redes, como roteadores ou switches durante períodos de congestionamento. Pacotes são mantidos nas filas para processamento posterior. Depois que está sendo processado pelo roteador, os pacotes, em seguida, são enviados para seu destino com base na prioridade (*IP Precedence, 802.1XP*) [54].

- ✓ Permite organizar as filas e servir classes de tráfego diferentemente de outras classes de tráfego;

Esta técnica oferece por outro lado, algumas limitações das quais a seguir destacamos as principais:

- ✓ Se ocorrer uma grande quantidade de tráfego de alta prioridade, o tráfego de baixa prioridade pode sofrer atrasos excessivos;
- ✓ Pode ocorrer estouro de capacidade das filas de fluxo de baixa prioridade;
- ✓ Um fluxo de alta prioridade mal comportado pode causar atraso e jitter em outro fluxo dentro da mesma fila. PQ não é uma solução para atender a limitação da fila FIFO com relação a favorecimento do tráfego UDP.

13.2.4.3 - Disciplina FQ - Enfileiramento Justo (*Fair Queuing*)

Como um *upgrade* ao algoritmo PQ, foi proposto o algoritmo de enfileiramento FQ, objetivando proporcionar métodos de tratamento diferenciados para os fluxos, em comparação ao PQ. Entretanto, este algoritmo não permite o tratamento diferenciado entre os fluxos, pois existe o tratamento uniforme entre todos os fluxos. Desta forma este algoritmo propõe-se lidar de forma mais eficiente com os notórios problemas de falta de recursos para algumas classes de tráfegos em contradição ao PQ.

Dessa forma o algoritmo FQ cria uma fila para cada fluxo e todos são tratados de forma uniforme, o que leva a entender que todos os fluxos possuem um volume de recursos previamente reservado, não podendo, contudo, consumir para além daquilo que fora especificamente determinado. Repare-se na Figura 69 a seguir, que exemplifica as filas específicas para cada tráfego mapeado pelo algoritmo FQ, característica muito diferente do PQ, ilustrado na Figura 68 acima. É criada, assim, para cada novo fluxo uma nova fila que será alocada apenas para um determinado tráfego de forma exclusiva. Com isto, quaisquer pacotes que chegam à interface do roteador serão classificados e direcionados para as respectivas filas previamente determinadas.

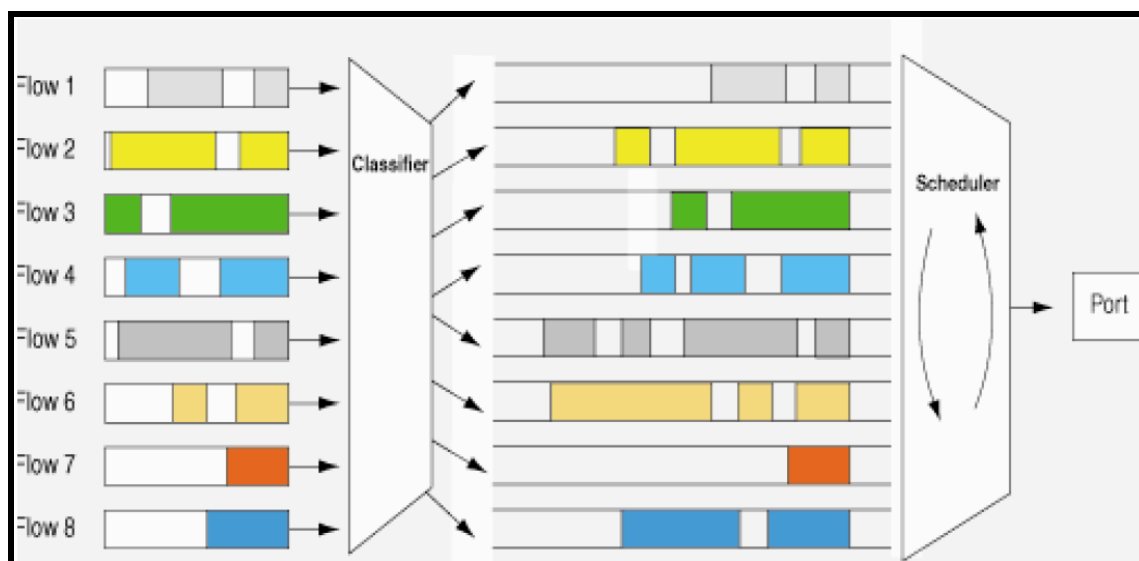


Figura 69 - Técnica de Enfileiramento Justo (FQ) [53].

O escalonador (*Scheduler*) visita cada fila, periodicamente, enviando a mesma quantidade de pacotes de cada fila, permitindo dessa forma, uma distribuição equitativa para a banda entre as classes [53]. As filas serão servidas de um pacote cada vez seguindo a ordem *Round-Robin*.

13.2.4.4 - Disciplina WFQ (*Weighted Fair Queuing*)

A disciplina de escalonamento WFQ foi desenvolvida para, justamente, suprir as limitações da disciplina FQ. A WFQ suporta fluxos com diferentes requisitos de largura de banda, atribuindo a cada fila um “peso” que assegura a diferença de banda por porta de saída. A WFQ também suporta pacotes de tamanhos variáveis. Assim, fluxos com pacotes maiores não locam mais banda que os fluxos de pacotes menores, o que a torna bastante interessante. A WFQ possui um classificador que classifica os fluxos de chegada e os insere em filas (FIFO) que podem ter larguras de bandas diferentes. O classificador também calcula e etiqueta cada pacote com um número diferente denominado “*Finish Time*”. O “*Finish Time*” representa a ordem com que os pacotes devem ser retirados das filas e encaminhados. Este é calculado a partir da taxa de bit de saída, do número de filas ativas, do peso relativo de cada fila e do tamanho do pacote. O escalonador verifica nas cabeças das filas qual delas possui o pacote com o menor *Finish Time*.

O pacote que tiver o menor número é retirado da fila e encaminhado para a saída [44],[65], conforme mostra a Figura 70 a seguir - WFQ tenta classificar e intercalar

tráfego por fluxo e, em seguida, enfileira-o de acordo com o volume de tráfego no fluxo.

Para esta disciplina é importante seleccionar um comprimento de enfileamento de mensagens mais adequado possível, pois, configurar um comprimento de fila inadequadamente, pode resultar em descarte de pacotes. Se o comprimento da fila for muito longo, pode introduzir, portanto, uma quantidade inaceitável de latência e *Round-Trip Time* (RTT) e isso prejudicaria sessões do protocolo de transporte ponto a ponto como o TCP (*Transmission Control Protocol*) estourando o tempo limite das sessões [54].

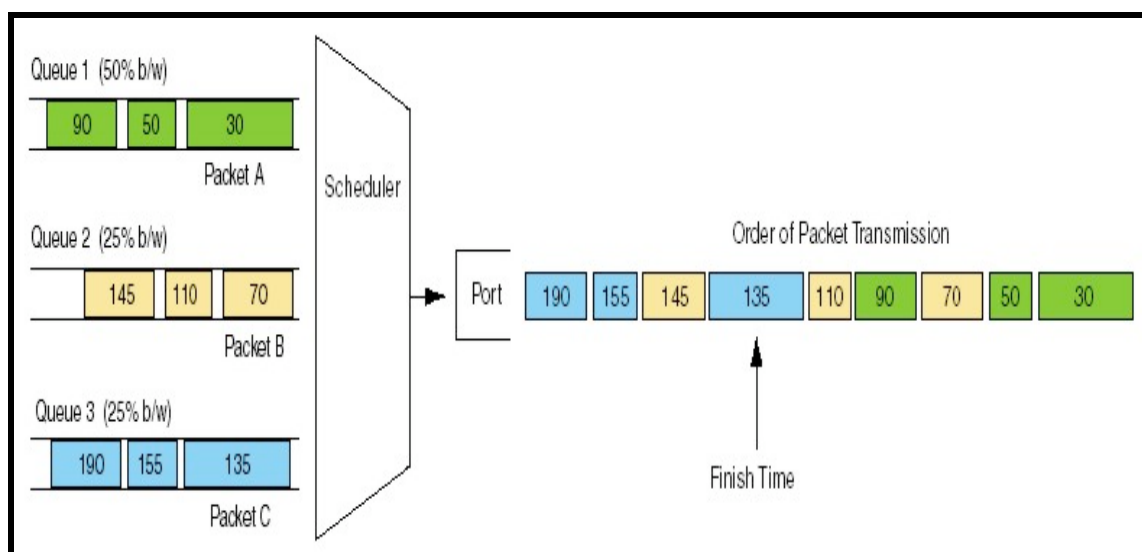


Figura 70 - Disciplina WFQ (Weighted fair queuing)

Percebe-se ainda que a Figura 70 ilustra o funcionamento do algoritmo WFQ, com três filas cada qual com diferentes percentagens de banda: uma de 50% e duas de 25%. Os diversos pacotes que chegam ao roteador são classificados e remetidos para as filas correspondentes. Porém, antes de se realizar a transmissão o escalonador calcula e assinala os tempos de chegada dos respectivos pacotes. A ordem de transmissão utilizada foi calculada na ordem crescente dos valores do tempo de chegada. [53].

A disciplina do tipo WFQ oferece as seguintes vantagens:

- ✓ A WFQ provê proteção para cada classe de serviço assegurando um mínimo de largura de banda independente do comportamento de cada classe.

As principais limitações são:

- ✓ A implementação é feita apenas em software e não em hardware;

- ✓ Fluxo mal comportado pode impactar no desempenho de outros fluxos na mesma classe;
- ✓ Algoritmo complexo;

13.2.4.5 - Disciplina WRR (*Weighted Round Robin*)

A disciplina de escalonamento WRR também conhecida por CBQ foi desenvolvida para suprir limitações da disciplina FQ e PQ. O WRR supre as limitações do FQ suportando fluxos com diferentes requisitos de largura de banda. Com o WRR, cada fila pode ser atribuída com diferentes percentagens de largura de banda de saída. O WRR supre as limitações do FQ assegurando que tráfego de baixa prioridade não seja prejudicado. Com o WRR, no mínimo um pacote é removido de cada fila a cada *round* [55]. De acordo com a Figura 71 a seguir o WRR primeiro classifica os pacotes que chegam em várias classes de serviço (exemplo: tempo real, interativo, transferência de arquivos, etc...) e em seguida insere os pacotes nas filas dedicadas a cada classe de serviço.

Cada fila é servida por um ordenador *Round Robin (RR)*. O WRR suporta a alocação de diferentes quantidades de largura de banda para diferentes classes de serviços, ou seja, permite que uma fila com largura de banda maior envie mais que um único pacote cada vez que é visitada durante um ciclo de serviço, ou permite que cada fila envie um pacote cada vez que é visitada. Porém, uma fila com maior largura de banda pode ser visitada múltiplas vezes em um único ciclo de serviço [44],[53].

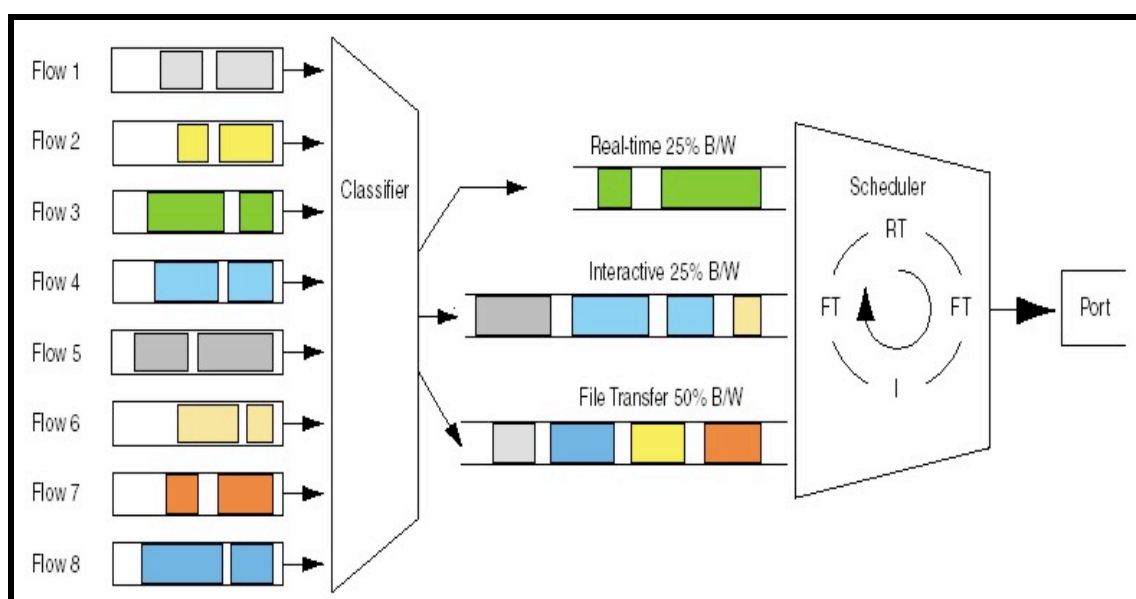


Figura 71 - Disciplina WRR (*Weighted Round Robin*) [53].

A disciplina do tipo WRR oferece as seguintes vantagens:

- ✓ Pode ser implementado em hardware;
- ✓ Provê um controle sobre cada porcentagem de largura de banda de saída;
- ✓ Assegura que todas as CoS tenham acesso a uma largura de banda de saída configurada;

A principal limitação é:

- ✓ Provê uma correta porcentagem de largura de banda de saída apenas se os pacotes inseridos em todas as filas forem do mesmo tamanho.

13.2.4.6 - Disciplina DWRR (*Deficit Weighted Round Robin*) ou DRR.

O DWRR foi desenvolvido para suprir as limitações dos algoritmos de escalonamento WRR e WFQ. O DWRR supre as limitações do WRR através de uma distribuição de largura de banda de saída justa, para filas que contenham pacotes de tamanhos variáveis. O DWRR supre as limitações do WFQ reduzindo a complexidade computacional do algoritmo e também por permitir a sua implementação em hardware, o que possibilita o uso de interfaces de alta velocidade [53], [55].

No DWRR cada fila é configurada com vários parâmetros:

- ✓ Um *Weight* (w) define a porcentagem de largura de banda de saída alocada a cada fila;
- ✓ Um *Deficit Counter* (DC) especifica o número total de bytes ou bits que uma fila pode transmitir cada vez que é visitada pelo escalonador. Se o tamanho do pacote for maior do que o DC , este último é creditado no saldo da fila para o próximo *round* (r) onde é feita uma nova comparação;
- ✓ Um *Quantum* (Q) de serviço que é proporcional ao peso da fila e expresso em bytes;
- ✓ O DC é incrementado de um Q cada vez que a fila é visitada pelo escalonador;

Nota sobre outras considerações:

O DC para uma fila é incrementado pelo Q cada vez que a fila é visitada pelo escalonador. Se $Q[u] = 2 * Q[y]$, então a fila “ u ” receberá o dobro de banda que a fila y quando as duas filas estiverem ativas. No algoritmo DWRR clássico, o escalonador

visita cada fila não vazia e determina o número de bytes do pacote da cabeça da fila, então:

- ✓ A variável DC é incrementada do valor Q ;
- ✓ Se o valor do pacote da cabeça da fila for maior que a variável DC então o escalonador mover-se-á para a próxima fila;
- ✓ Se o tamanho do pacote da cabeça da fila for menor ou igual a variável DC , então esta será decrementada do tamanho do pacote e este será transmitido pela porta de saída;
- ✓ O escalonador continua retirando os pacotes e decrementando a variável DC do tamanho do pacote transmitido até que o tamanho do pacote da cabeça da fila seja maior que a variável DC ou que a fila esteja vazia;
- ✓ Se a fila estiver vazia o valor DC receberá zero.

Quando isso ocorre o escalonador move-se para a próxima fila não vazia. Assim, a Figura 72 a seguir ilustra a utilização do algoritmo DWRR, utilizando o quantum de 1000 para a fila 1, *quantum* de 500 respectivamente para as duas restantes filas [53][54].

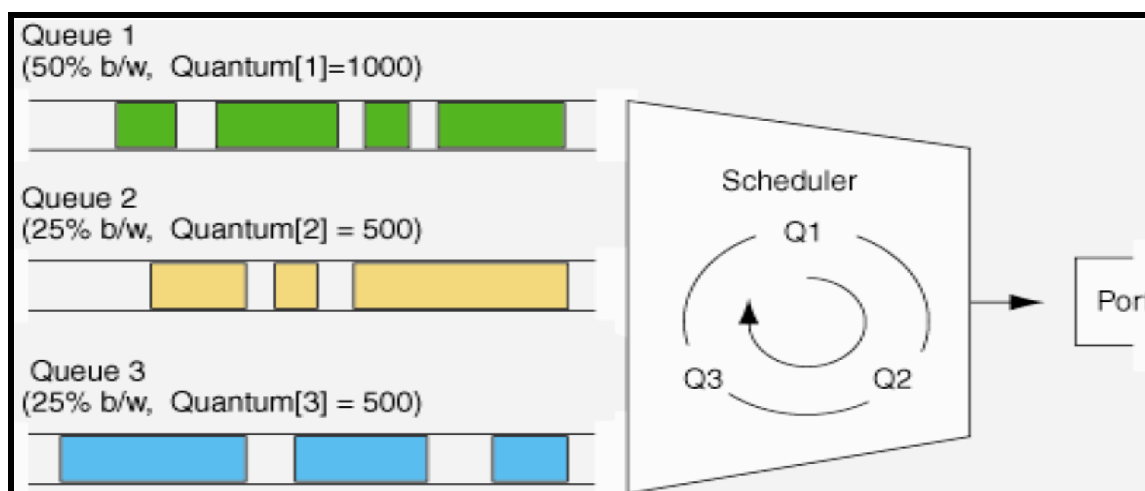


Figura 72 - Funcionamento do Algoritmo Deficit Weighted Round Robin [53]

O DWRR tem as seguintes vantagens:

- ✓ Supera as limitações do WRR provendo um controle preciso da percentagem de largura de banda de saída alocada para cada classe de serviços quando se encaminham pacotes de tamanhos variáveis;

-
- ✓ Supera as limitações do PQ assegurando que todas as classes de serviços tenham acesso a uma quantidade de largura de banda de saída configurada;
 - ✓ A implementação do algoritmo é relativamente simples.
 - ✓

A principal limitação é:

- ✓ Fluxos mal comportados podem impactar no desempenho de outros fluxos dentro da mesma classe de serviços.

Fim das considerações sobre a QoS –*DiffServ* e fecha com isso a Dissertação.

FIM!.

*“O homem esquece, mais facilmente a morte do pai
do que a perda do patrimônio” – Maquiavel*